MAR 1 7 1982

Y3.N88:25/2515/v.2

NUREG/CR-2515
SAND81-7229/II
AN
Printed December 1981

COMPLETED
640

CONTRACTOR REPORT

ORIGINAL

Crystal River-3 Safety Study
Volume II – Appendices

A. A. Garcia, Principal Investigator
R. T. Liner, P. J. Amico, E. V. Lofgren
Science Applications, Inc.
7315 Wisconsin Ave, Suite 1200 W
Bethesda, MD 20814

Prepared for
U. S. NUCLEAR REGULATORY COMMISSION

I

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

Available from
GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
and
National Technical Information Service
Springfield, Virginia 22161

SAI-002-81-BE

NUREG/CR-2515/II of II
SAND81-7229/II of II

CRYSTAL RIVER-3 SAFETY STUDY

VOLUME II

APPENDICES

1 December 1981

Prepared by:
Science Applications, Inc.
7315 Wisconsin Avenue, Suite 1200W
Bethesda, Maryland 20814

Principal Investigator:
A. A. Garcia

Principal Authors:
R. T. Liner
P. J. Amico
E. V. Lofgren

Funded by
Division of Risk Analysis
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
Under Memorandum of Understanding DOE 40-550-75
NRC FIN No. A1241 (Sandia)
A6296 (EG&G)

TABLE OF CONTENTS

Page

VOLUME I - MAIN REPORT

Foreword . . . . I-i

Acknowledgements . . . . I-ii

Table of Contents . . . . I-iii

List of Figures . . . . I-vi

List of Tables . . . . I-viii

Glossary . . . . I-x

1.0 INTRODUCTION 1-1

2.0 SUMMARY OF RESULTS 2-1

- 2.1 Frequency of Radioactivity Releases 2-1
- 2.2 Dominant Sequences 2-3
- 2.3 Functional and System Dependencies 2-16
- 2.4 Limitations of the Analysis 2-21

3.0 GENERAL PLANT DESCRIPTION 3-1

- 3.1 Reactor Coolant System (RCS) 3-6
- 3.2 Reactor Protection System (RPS) 3-6
- 3.3 Engineered Safeguards Actuation System (ESAS) 3-7
- 3.4 Engineered Safeguards Systems 3-7
  - 3.4.1 Emergency Core Cooling System (ECCS) 3-8
  - 3.4.2 Reactor Building Cooling and Spray Systems 3-11
- 3.5 Emergency Feedwater System (EFS) 3-12
- 3.6 Emergency Auxiliary Systems 3-12
  - 3.6.1 Electric Power 3-13
  - 3.6.2 Emergency Cooling Systems 3-13
- 3.7 Connections Between CR-3 and Coal-Fired Units 1 and 2 . . 3-15

[redacted]

TABLE OF CONTENTS

Page

4.0 EVENT TREES 4-1

4.1 Initiating Events 4-1
  4.1.1 Transient Initiators 4-2
  4.1.2 LOCA Initiators 4-3
4.2 Transient Event Tree 4-4
4.3 LOCA Event Tree 4-13
4.4 Special Events 4-19
  4.4.1 Interfacing Systems LOCA (Event V) 4-19
  4.4.2 Vessel Rupture 4-21
  4.4.3 Steam Generator Tube Rupture 4-24
4.5 Containment Failure Modes 4-24
4.6 Radioactive Release Categories 4-27

5.0 FAULT AND EVENT TREE QUANTIFICATION PROCEDURES 5-1

5.1 Analytical Methods for Estimating Primary Event Probabilities 5-1
  5.1.1 Fault Tree Development 5-1
  5.1.2 Quantification Data Base 5-4
  5.1.3 Evaluation of Hardware Faults 5-11
  5.1.4 Evaluation of Human Faults 5-11
  5.1.5 Evaluation of Common-Cause Faults 5-12
  5.1.6 Evaluation of Test and Maintenance Outages 5-13
  5.1.7 Evaluation of Interfacing System Faults 5-14
  5.1.8 Evaluation of System Unreliability During Recirculation 5-15
5.2 Fault Tree Organization and Structure 5-17
  5.2.1 A Fault Tree Hierarchy 5-18
  5.2.2 System and Subsystem-Level Faults 5-20
  5.2.3 Functional Level Faults 5-27
  5.2.4 Fault Tree Quantification Tables 5-29

[redacted]

TABLE OF CONTENTS

Page

5.3 Sequence Analysis 5-34
  5.3.1 Boolean Reduction of Event Tree Sequences 5-34
  5.3.2 Initiating Event Frequencies 5-37
  5.3.3 Probabilities for Special Events in the Transient Event Tree 5-38
  5.3.4 Analysis of ATWS Sequence 5-40
  5.3.5 Containment Failure Probabilities 5-46
  5.3.6 Accident Sequence Analysis Results 5-48
5.4 Analysis of Selected Operator Faults 5-66

VOLUME II - APPENDICES

Table of Contents . . . . II-i
Glossary . . . . II-iv
Introduction II-1
Appendix A - Reactor Protection System (RPS) A-1
Appendix B - Engineered Safeguards Actuation System (ESAS) B-1
Appendix C - DC Power System C-1
Appendix D - Class I.E. AC Power System D-1
Appendix E - Nuclear Services Closed Cycle Cooling System (NSCCCS) E-1
Appendix F - Decay Heat Closed Cycle Cooling System (DHCCCS) . . . F-1
Appendix G - High Pressure Injection and Recirculation System . . G-1
Appendix H - Core Flood System (CFS) H-1
Appendix K - Low Pressure Injection and Recirculation System . . K-1
Appendix L - Reactor Building Emergency Cooling System (RBECS) . . L-1
Appendix M - Reactor Building Spray System (RBSS) M-1
Appendix N - Reactor Building Isolation System (RBIS) N-1
Appendix P - Emergency Feedwater System (EFS) P-1

GLOSSARY OF ABBREVIATIONS

A/E	Architect Engineer
ATWS	Anticipated Transient Without Scram
BWST	Borated Water Storage Tank
CRA	Control Rod Assembly
CFT	Core Flood Tanks
CR-3	Crystal River Unit 3
CRDM	Control Rod Drive Mechanism
DHCCCS	Decay Heat Closed Cycle Cooling System
DHCWS	Decay Heat Services Cooling Water System
DHSWS	Decay Heat Sea Water System
ECCS	Emergency Core Cooling System
ECF	Emergency Cooling Functionability
ECI	Emergency Coolant Injection
ECR	Emergency Coolant Recirculation
EFS	Emergency Feedwater System
EPRI	Electric Power Research Institute
ESAS (ESFAS)	Engineered Safeguards Actuation System
FSAR	Final Safety Analysis Report
HE	Heat Exchanger
HP, HPI, HPR	High Pressure (Injection) (Recirculation)
ICS	Integrated Control System
LOCA	Loss of Coolant Accident
LOSP	Loss of Offsite Power
LP, LPI, LPR	Low Pressure (Injection) (Recirculation)

GLOSSARY OF ABBREVIATIONS (CONT.)

MFW	Main Feedwater
MOV	Motor Operated Valve
NC, N.C.	Normally Closed
NO, N.O.	Normally Open
NPSH	Net Positive Suction Head
NRC	Nuclear Regulatory Commission
NSCWS	Nuclear Service Cooling Water System
NSCCCS	Nuclear Services Closed Cycle Cooling System
NSSS	Nuclear Steam Supply System
NSSWS	Nuclear Services Sea Water System
OTSG	Once Through Steam Generator
PAHR	Post Accident Heat Removal
PARR	Post Accident Radioactivity Removal
PCS	Power Conversion System
PORV	Power Operated Relief Valve
RB(E)CS	Reactor Building (Emergency) Cooling System
RBIC	Reactor Building Isolation and Cooling
RBIS	Reactor Building Isolation System
RBSS, RBSI, RBSR	Reactor Building Spray System (Injection) (Recirculation)
RCS	Reactor Coolant System
RPS	Reactor Protection System
RSS	Reactor Safety Study (WASH-1400)
RSSMAP	Reactor Safety Study Methodology Applications Program
S/RV	Safety/Relief Valve

APPENDICES: SYSTEM DESCRIPTION AND FAULT TREE ANALYSES

INTRODUCTION

This Volume consists of a collection of Appendices of system descriptions and fault tree analyses, including the unavailability quantifications for all systems designed to mitigate accident consequences and the auxiliary systems which support the "front-line" systems. The various systems are individually presented in Appendices A through P, which immediately follow the generic descriptive material below.
This introductory material and discussion is provided to assist the reader in understanding the overall structure of the CR-3 Safety Study and the organization and format of the individual Appendices. It is also intended to explain what kind of information and results the reader can expect to find in these Appendices.

The flow chart presented in Figure II.1 shows the main steps involved in the risk assessment of CR-3. It also shows the structure of the fault tree analysis contained in a typical Appendix[1]. The following discussion is a step-by-step account of the quantification process for the fault tree analysis of each system. The steps are keyed to the numbers shown in diamonds in Figure II.1.

STEP ⟨1⟩ The starting point was the collection, review and study of plant information to gain a thorough understanding of the system designs and capabilities, and interactions between systems.

---

[1] In the following discussion, a typical Appendix is generally referred to as Appendix X.

The main sources of information were[2]:

- Plant Design Information - CR-3 FSAR (II-1)[3] System Drawings (e.g., P&IDs, One Line Diagrams, Elementaries), FPC System Descriptions, etc.

- Technical Specifications (II-2)

- Plant Visit - gain familiarity with the equipment layout (possibly common mode failures due to common location); extensive discussions with plant personnel about plant operation, test and maintenance practices, operating experience, etc.

- Plant Procedures - Examples of procedures used are: Operating-, Maintenance-, Surveillance-, Emergency-Procedures, etc. These procedures (1) provide insight into the general plant operation and (2) support the operators during abnormal occurrences (especially the Emergency-Procedures). The procedures are also important to the quantification effort because they describe what is done to the various plant systems and how it is done.

- Expert Opinion and Experience - Collect information on plant and systems behavior, containment failure modes, etc., from experts available at FPC, B&W, NRC, and National Laboratories.

Section X.1, the first section of each appendix, summarizes the information collected during Step ⟨1⟩. The intent of this section is to convey to the reader all information necessary to follow the system's fault tree quantification.

STEP ⟨2⟩ With the information gathered in Step ⟨1⟩ the construction of the event trees, based on the system functions required for accident mitigation, can begin.

STEP ⟨3⟩ The success requirements for each event tree heading (or function) are determined in this step. Where possible, the requirements are defined in terms of systems.

---

[2] Not shown in the chart are the many iterations and exchanges among the various sources and other project personnel throughout the duration of this project.

[3] Numbers shown in parentheses in the text, e.g., (II-1) indicate references.

STEP ⟨4⟩ At this point, all the systems, including the supporting systems, contributing to the mitigation of an accident are shown. Special studies, performed in parallel with the steps described thus far may allow exclusion of certain systems from detailed fault tree anlysis. These special studies and their conclusions are discussed in Volume I.

STEP ⟨5⟩ Detailed fault trees for all the systems selected in Step ⟨4⟩ are constructed. The definition of the top event for each tree is based on the success requirements developed in Step ⟨3⟩. The detailed fault trees are developed for each system to a level of detail sufficient to identify possible common mode or common cause failures.

STEP ⟨6⟩ Simplified fault trees are developed from the detailed trees of Step ⟨5⟩. The basic fault elimination criteria for the simplification process results in simplified trees containing only single active and passive faults, double active faults, test and maintenance outages, and common mode failures. The simplification process eliminates other faults, including those whose contributions to the top event is neglibile (on the basis of of relative probability values) compared to other contributors. Thus the detailed trees are "pruned" to simplified trees which contain only the dominant cutsets, i.e., failure combinations, leading to the occurrence of the top event.

The simplified fault trees are presented in Section X.2 of each appendix, together with the top event definition and any assumptions made for the development of the detailed trees.

Sections X.1 and X.2 complete the basic information necessary to proceed to the fault tree quantification process presented in Section X.3. The first subsection, X.3.1, discusses the system reliability characteristics. The results of the system quantification are summarized by highlighting the dominant contributors to the system's unavailability.

Each of the following steps discussed is presented in the Appendix either in table form or as a figure(s) in the logical sequence of development. Extensive use of notes, attached to the tables and figures as required, was made to explain and substantiate entries in the tables and figures.

Two distinct phases in a post accident environment exist: the injection phase and, in most cases, the recirculation phase. Sections X.3.2 and X.3.3 contain the quantification for the two post-accident phases. The steps in the quantification process, which are the same for both phases, are discussed below. The reason for the construction of modularized fault trees is discussed in Section 5.1 of Volume I.

STEP ⟨7⟩ The appropriate event tree heading success requirements developed in Step ⟨3⟩, and presented in Volume I, Tables 4.4 and 4.6, formed the basis for the definition of the success requirements for the individual systems.

STEP ⟨8⟩ The top events for the modularized fault trees are defined in this step. The selection of top events for systems and/or system trains is based on Step ⟨7⟩. Intermediate top events are frequently defined for (1) portions of system trains which are shared with other systems, and (2) for convenience of analysis.

STEP ⟨9⟩ Construction of the modularized fault trees consists of grouping the faults which appear on the simplified fault tree, step ⟨6⟩, by type into modules, e.g., single hardware faults, system interfacing faults, etc. The construction of the modules is also governed by the requirements of the sensitivity analysis to be performed. Some modules have to be separated to accommodate events of different sensitivity types. The event sensitivity types are discussed in Step ⟨11⟩.

STEP 10 The Boolean equations, representing the modularized fault trees, are developed in this step. The equations are Boolean reduced by hand whenever practicable; otherwise a Boolean reduction computer code, such as WAMCUT (II-3), is used. All crossterms prohibited by Technical Specifications are eliminated from the reduced equation since the crossterms represent simultaneous outage of both trains of a redundant two train system due to test, maintenance, or any combination thereof. (It is assumed that the plant does not intentionally violate applicable Technical Specifications.) The Boolean equations are input to the event tree sequence analysis.

STEP 11 This step represents the quantification of each module appearing on the modularized fault tree, The WASH-1400 data base (II-4) is used in general; in a few instances other data sources are used as indicated in the notes to the quantification tables.

The calculation of maintenance and test outages is discussed in Section 5.1 of Volume I and is, in several cases, contained in the notes. Otherwise, standard methods such as those shown in WASH-1400 (II-4), and IEEE Standard 352 (II-5), for example, were used to calculate unavailabilities.

A "D" in the "failure rate" column of the quantification tables means "demand", and "ε" means negligible contribution. The code for the abbreviations used for the sensitivity type (or subgroup) in the column labeled "SENS." is as follows:

O - Operator Error (defined in Volume I, Section 5.1)

H - Human Error (defined in Volume I, Section 5.1)

B - Hardware Coupling (defined in Volume I, Section 5.1)

M - Maintenance Outage

S - Selected Components (e.g., components in severe environment)

The last table in Section X.3.2 or X.3.3 is the quantification summary and contains the event unavailability point estimates. Steps ⟨7⟩ through ⟨11⟩ are repeated for systems required to operate during the recirculation phase. Step ⟨11⟩ completes the input required to perform the event tree sequence analysis.

Appendices A and B do not follow exactly the step-by-step outline above. The simplified fault tree is used in a slightly modified form instead of a modularized fault tree for the quantification of the Reactor Protection System (RPS) in Appendix A, and the simplified fault trees are used for the quanfication of the Engineered Safeguards Actuation System (ESAS) in Appendix B.

References

II-1 Florida Power Corporation, "Crystal River Unit 3 Nuclear Generating Plant Final Safety Analysis Report," Docket 50-302, 1971 (as amended through March 26, 1976).

II-2 Technical Specifications; Appendix A to the Operating License for Crystal River-Unit 3.

II-3 R. C. Erdmann, F. L. Leverenz, H. Kirch and G. S. Lellouche, Electric Power Research Institute, "WAMCUT, A Computer Code for Fault Tree Evaluation," EPRI NP-803, 1978.

II-4 U. S. Nuclear Regulatory Commission, "Reactor Safety Study-An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," Appendix III, WASH-1400 (NUREG-75/014), October 1975.

II-5 Institute of Electrical and Electronics Engineers, Inc., "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems," IEEE Std 353-1975, April 1975.

BEST DOCUMENT AVAILABLE

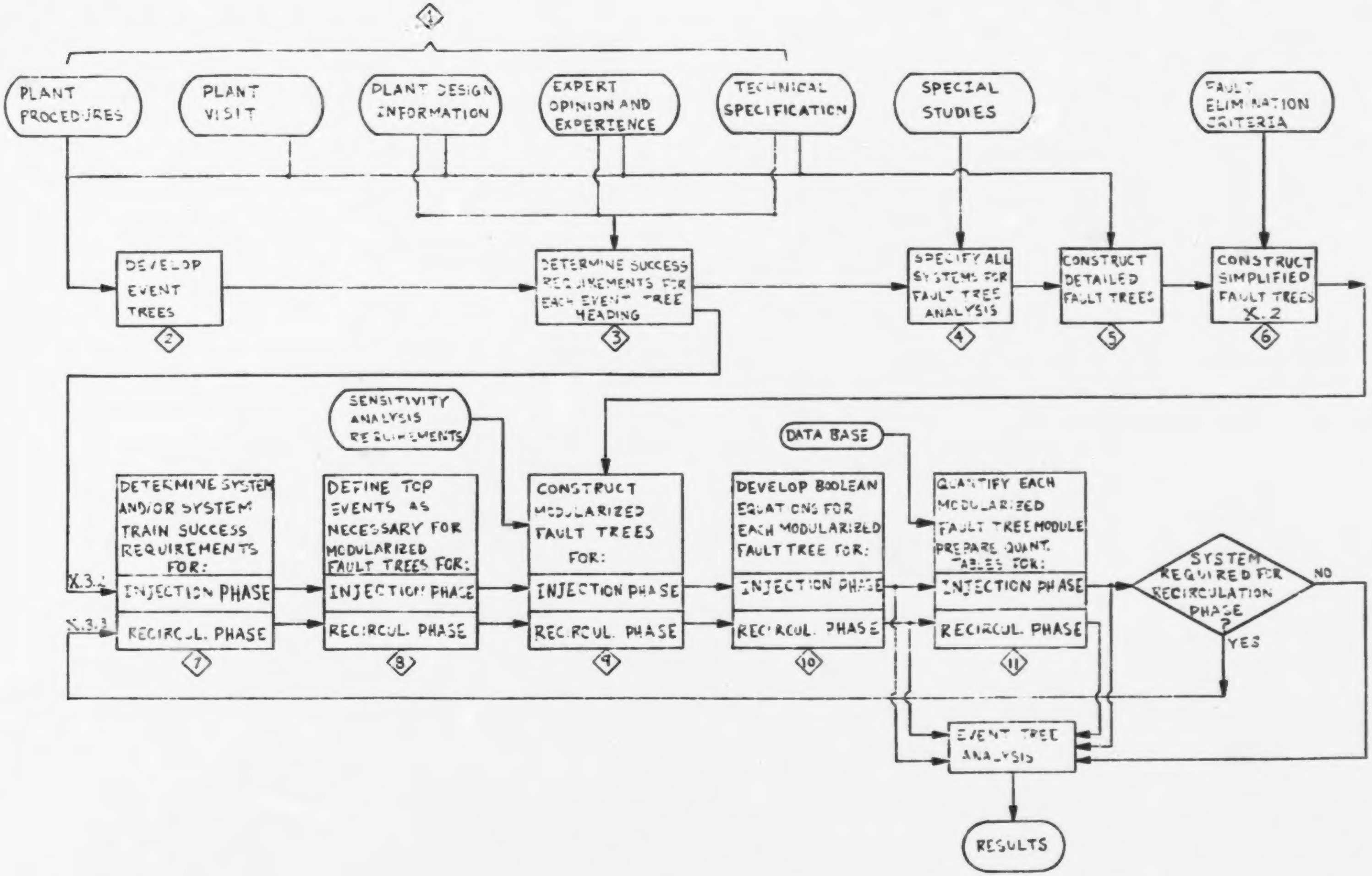

1
PLANT PROCEDURES
PLANT VISIT
PLANT DESIGN INFORMATION
EXPERT OPINION AND EXPERIENCE
TECHNICAL SPECIFICATION
SPECIAL STUDIES
FAULT ELIMINATION CRITERIA
DEVELOP EVENT TREES
2
DETERMINE SUCCESS REQUIREMENTS FOR EACH EVENT TREE HEADING
3
SPECIFY ALL SYSTEMS FOR FAULT TREE ANALYSIS
4
CONSTRUCT DETAILED FAULT TREES
5
CONSTRUCT SIMPLIFIED FAULT TREES X.2
6
SENSITIVITY ANALYSIS REQUIREMENTS
DATA BASE
X.3.2
X.3.3
DETERMINE SYSTEM AND/OR SYSTEM TRAIN SUCCESS REQUIREMENTS FOR:
INJECTION PHASE
RECIRCUL. PHASE
7
DEFINE TOP EVENTS AS NECESSARY FOR MODULARIZED FAULT TREES FOR:
INJECTION PHASE
RECIRCUL. PHASE
8
CONSTRUCT MODULARIZED FAULT TREES FOR:
INJECTION PHASE
RECIRCUL. PHASE
9
DEVELOP BOOLEAN EQUATIONS FOR EACH MODULARIZED FAULT TREE FOR:
INJECTION PHASE
RECIRCUL. PHASE
10
QUANTIFY EACH MODULARIZED FAULT TREE MODULE PREPARE QUANT. TABLES FOR:
INJECTION PHASE
RECIRCUL. PHASE
11
SYSTEM REQUIRED FOR RECIRCULATION PHASE ?
NO
YES
EVENT TREE ANALYSIS
RESULTS

Figure II.1 Main Steps Involved in the Risk Assessment of Crystal River-3

APPENDICES

SYSTEM DESCRIPTIONS AND FAULT TREE ANALYSES

APPENDIX A

REACTOR PROTECTION SYSTEM (RPS)

APPENDIX A REACTOR PROTECTION SYSTEM (RPS)

A.1 SYSTEM DESCRIPTION AND OPERATION

The Reactor Protection System (RPS) monitors parameters related to reactor operation and trips the reactor by control rod insertion into the core to protect the core against fuel rod cladding damage. In addition, it protects against reactor coolant system damage from high system pressure through rod insertion, thereby limiting energy input to the system.

A.1.1 SYSTEM DESCRIPTION

The RPS consists of control rod assemblies (CRA), circuit breakers, instrumentation and electronic logic. The logic, in response to input signals from the instrumentation, shuts down the reactor by removing power from the control rod drive mechanism (CRDM) motors. The control rods then drop into the core under the influence of gravity. A schematic of the RPS is shown in Figure A.1.

There are a total of 69 CRA's, arranged in eight groups including four safety groups, three regulating groups and one axial power shaping group. The rod drive control system includes (1) five identical, dual channel DC supplies which power the regulating and axial power shaping groups and (2) two DC holding power supplies which power the safety groups. The DC supplies are fed from two 480VAC, 3ø sources; i.e., a main bus and a secondary bus. Two primary breakers (A,B), two secondary breakers (C,D), and contactors (E,F) interrupt power to the CRA drive motors when a trip is commanded.

The trip logic includes four identical channels, each consisting of logic circuits and trip relays, which maintain the trip breakers and contactors energized under normal operating conditions. In response to input signals from sensors (See Table A.1), the channel logic deenergizes associated trip relays which in turn deenergize the trip breakers and contactors thereby removing power to the CRDM motors and causing the regulating and safety CRA's (61) to drop into the core. The axial power shaping rods do not drop into the core when their associated drive motors are deenergized.

CONTROL ROD ASSEMBLY

The CRA includes 16 control rods, mounted in a stainless-steel spider, and a control rod drive mechanism. The CRDM, which positions the CRA in the reactor core, is a non-rotating translating lead screw coupled to the CRA. The screw is driven by split roller nut assemblies which are rotated magnetically by a motor stator located outside the pressure boundary. For rapid insertion, power is removed from the drive motor causing the nut halves to separate and release the screw and CRA which then drop into the reactor core under the influence of gravity.

The CRAs are arranged into groups at the control rod drive control system patch panel. Typically twenty-eight CRAs are assigned to the regulating groups (Groups 5,6,7,8) while forty-one CRAs are assigned to the safety rod groups (groups 1,2,3,4). Group 8 includes eight axial power shaping rod assemblies which do not drop into the core when power is removed from their drive motors during a reactor trip.

The rod drive control system (RDC), which is shown in Figure A.2 consists of (1) drive motor DC power supplies, (2) system control logic, and (3) trip breakers and contactors. The DC power system includes four group power supplies. Identical power supplies are used for the regulating groups and the auxiliary power supply. The DC power supplies are fed from two 480VAC, 3ϕ sources; i.e., a main bus and a secondary bus.

The system logic encompasses those functions which command control rod motion in the manual or automatic modes of operation, including CRD sequencing, safety and protection features, and the manual trip function. Major components of the logic system are the Operator's Control Panel, CRA position indication panels, automatic sequencer, and relay logic. Switches are provided at the operator's control panel for selection of the desired rod control mode. Control modes are: (1) Automatic mode -- where CRA motion is commanded by an integrated control system; and (2) Manual mode -- where CRA motion is commanded by the operator. Manual control permits operation of a single CRA or a group of CRAs. Alarm lamps on the RDC panel alert the operator to the systems status at all times. The group 8 control rods can only be controlled manually, even when the remainder of the system is in automatic control. The sequence section of the logic system utilizes rod position signals to generate control interlocks which regulate group withdrawal and insertion. The sequencer operates in both automatic and manual modes of reactor control, and controls the regulating groups only. Analog position signals are generated by the read switch matrix on the CRA, and an average group position is generated by an averaging network. This average signal serves as an input to electronic trip units which are activated at approximately 25 and at 75 per cent of group withdrawal. Two bistable units are provided for each regulating group. Outputs of these bistables actuate "enable" relays which permit the groups to be commanded in automatic or manual mode. The automatic sequencer circuit can control only CRA groups 5,6 and 7. The safety CRA groups, groups 1-4, are controlled manually, one group at a time. In addition, the operator must select the safety group to be controlled and transfer it to the auxiliary power supply before control is possible. There is no way in which the automatic sequencer can affect the operations required to move the safety CRA. Automatic insertion of rods can only be commanded by the integrated control system when the control rod drive system is in the automatic mode.

Positioning of regulating CRAs is accomplished by silicon controlled rectifier switching via a motor driven multichannel photo-optic encoder. The safety CRAs are positioned via the auxiliary power supply and maintained in the desired position by the holding power supplies.

Trip breakers and contactors are provided for removing power to the CRDM motors. The AC power feed breakers are of the three-pole, stored-energy type and are equipped with instantaneous undervoltage trip coils. Each AC feed breaker is housed in a separate metal clad enclosure. The secondary trip breakers are also of the stored-energy type with two parallel-connected instantaneous undervoltage trip coils consisting of two 2-pole breakers mechanically ganged to interrupt DC busses. All breakers are motor-driven-reset to provide remote reset capability. Each undervoltage trip coil is operated from the Reactor Protection System. The trip breakers are tested monthly.

TRIP LOGIC

The system shown in Figure A.1 consists of four identical channels, each terminating in a trip relay within a reactor trip module. The primary source of AC power for the RPS comes from four vital 120VAC buses, one for each protective channel. In the normal untripped state, each channel maintains the trip relay energized via the closed normally open (N/O) contacts of bistables associated with the various reactor sensors. Should any bistable become deenergized the trip relay deenergizes. Each trip relay has four N/O contacts, each controlling a logic relay in one reactor trip module. Therefore, each reactor trip module has four logic relays controlled by the four channels. The four logic relays combine to form a 2-out-of-4 coincidence network in each reactor trip module.

Manual trip may be accomplished from the control console by a trip switch. This trip is independent of the automatic trip system. Power from the control rod drive power breakers' undervoltage coils comes from the RT modules. The manual trip switches are between the reactor trip module output and the breaker undervoltage coils. Opening of the switches opens the lines to the breakers, tripping them. There is a separate switch in series with the output of each reactor trip module. All switches are actuated through a mechanical linkage from a single pushbutton.

Each channel is provided with two key-operated bypass switches, a channel bypass switch and a shutdown bypass switch. The channel bypass switch enables a channel to be bypassed without initiating a trip. Actuation of the switch initiates a visual alarm on the main console which remains in effect during any channel bypass. This switch is used to bypass one protective channel during on-line testing. Thus, during on-line testing the system will operate in 2-out-of-3 coincidences. An electric interlock circuit prevents placing two channels in bypass simultaneously. The use of the channel bypass key switch is under administrative control.

The shutdown bypass switch enables the power/imbalance/flow, power/RC pumps, low pressure, and pressure-temperature trips to be bypassed, allowing control rod drive tests to be performed after the reactor has been shutdown and depressurized below the low reactor coolant pressure trip point. Before the bypass may be initiated, a high pressure trip bistable - which is incorporated in the shutdown bypass circuitry - must be manually reset. The set point of the high pressure bistable (associated with shutdown bypass) is set below the low pressure trip point. If pressure is increased with the bypass initiated, the channel will trip when the high pressure bistable (associated with shutdown bypass) trips. The use of the shutdown bypass key switch is under administrative control.

Each of the four channels is physically separate and electrically isolated from the regulating instrumentation. The modules, logic, and analog equipment associated with a single protective channel are contained wholly within two Reactor Protection System cabinets. Within these cabinets, there is a meter for every analog signal employed by the protective channel, and a visual indication of the state of every logic element. At the top of one cabinet, and visible at all times, is a protective channel status panel. Lamps on this panel give a quick visual indication of the trip status of the particular protective channel and of the RT module associated with it. Additional lamps on the panel give visual indication of a channel bypass or a fan failure.

The RPS equipment is designed for continuous operation in a room environment of 40^{0}F to 110^{0}F and up to 75% relative humidity. All modules are designed for a 30^{0}F temperature rise inside the equipment cabinets over the ambient room conditions. Two 100% capacity fans with filter banks and chilled water coils, two 100% capacity central station type chilled water systems, and two 50% capacity outside air booster fans are provided for environmental control of the equipment area.

A.1.2 SYSTEM OPERATION

The coincidence logic contained in the RPS channel A controls trip breaker A in the control rod drive system, channel B controls breaker B, channel C controls breaker C and contactor E, and channel D controls breaker D and contactor F. The control rod drive circuit breaker combinations that initiate reactor trip include (1) AB, (2) ADF, (3) BCE, and (4) CDEF. This is a 1-out-of-2 twice logic. When any 2-out-of-4 channels trip, all reactor trip modules trip (deenergize) all control rod drive breakers and contactors. The four RPS channels trip whenever the reactor conditions tabulated in Table A.1 exist.

The use of 2-out-of-4 logic between protective channels permits a channel to be tested on-line without initiating a reactor trip. Maintenance to the extent of removing and replacing any module within a protective channel may also be accomplished in the on-line state without a reactor trip. Each logic channel is tested monthly. The RPS sensors are checked during each shift and are tested monthly. To prevent either the on-line testing or maintenance features from creating a means for unintentionally negating protective action, a system of interlocks initiates a protective channel trip whenever a module is placed in the test mode or is removed from the system. However, provisions are made to bypass any one protective channel (i.e., supply an input signal which leaves the channel in a non-tripped condition) for testing or maintenance. The test scheme for the reactor protective system is based upon the use of comparative measurements between like variables in the four protective channels, and the substitution of digital and analog test signals as required, together with measurements of actual protective function trip points. The test signals are provided from built-in test circuits in the logic instrumentation system. A digital voltmeter (not cabinet-mounted) is used for making accurate measurements of trip point and analog signal voltages.

Plant annunciator windows provide the operator with immediate indications of changes in the status of the reactor protective system.

The following conditions are annunciated for each reactor protective system channel:

- a. channel trip
- b. fan failure in channel
- c. channel on test
- d. shutdown bypass initiated
- e. manual bypass initiated

Any time a test switch is in other than the operate position, annunciator "c" will be lit and the associated protection channel will be tripped. Under this condition, annunciator "a" will be lit unless annunciator "e" is lit (i.e., the channel is bypassed).

TEST AND MAINTENANCE

Each RPS channel, including the associated instrumentation, reactor trip module (RTM), and CRD breaker and contactor, is demonstrated operable by performance of functional tests once each month.

Functional testing of each of the four channels requires approximately four hours to complete and is performed on a weekly rotation by different test personnel.*

---

*Per discussion with plant personnel.

Following are several notes related to test and maintenance.

Notes on Reactor Trip Module

- Prior to start of functional testing of the instrumentation and RTM associated with the particular channel under test, the channel is placed in bypass via the "Manual Bypass" switch located in the RTM. This reduces the RPS trip logic to a 2-out-of-3 system.
- When RTM is placed in bypass via manual bypass switch, indication of this condition is provided in the control room (RPS Panel).
- Operator can leave channel in bypass state but indication on RPS panel should alert operator. Same applies to inadvertent bypass.
- An electric interlock circuit prevents placing two channels in bypass simultaneously.
- Only one channel is permitted to be bypassed at any given time under administrative control.

Notes on Control Rod Drive (CRD) Power Train

- Functional testing of the CRD power train consists of causing the CRD breaker to trip. A jumper is momentarily placed across the trip coil of the breaker. The power train is restored to operational status by locally resetting the breaker.
- A breaker can be racked out for maintenance without channel trip.

Notes on Instrumentation

- If a reactor sensor requires maintenance to correct for a defect, the work will be done during a shutdown.
- Work can be performed on the circuitry of the instrumentation signal processing electronics (such as the power supply, signal conditioners, etc.), but the associated channel will probably be bypassed.
- Calibration errors in the signal processing electronics can result in a circuit being unavailable to trip the reactor. (Calibration is performed on each channel on a weekly rotation basis, by different personnel.)

Table A.1 Reactor Trip Summary

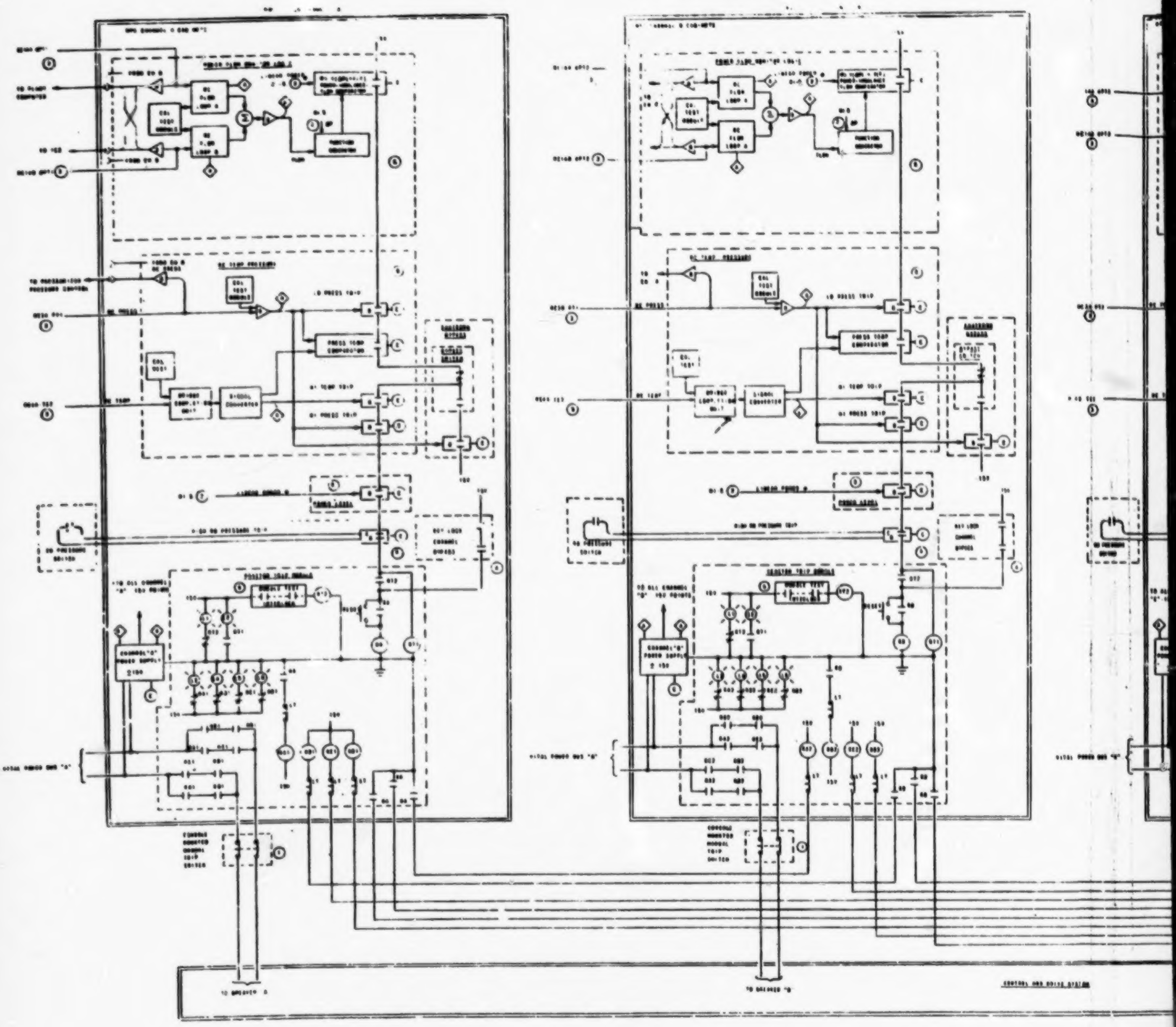
Trip Variable	No. of Sensors	Steady-State Normal Range	Trip Value or Condition for Trip
Overpower	4 flux sensors	2-100%	≥105.5% of rated power
Nuclear overpower based on flow and imbalance	4 two-section flux sensors, 8 ΔP flow	NA	1.045 times flow minus reduction due to imbalance
Reactor outlet temperature	4 temperature sensors	532-604 F	≥620F
Pressure/temperature	4 pressure sensors, 4 temperature sensors	Variable	$(16.25T - 7838) \geq P$[a]
Reactor coolant pressure	4 pressure sensors	2,090-2,220 psig	≥2,355 psig (high), ≤1,800 psig (low)
Reactor building pressure	4 pressure switches	0 psig	4 psig

---

[a] T is in F and P is in psig.

[redacted]

BEST DOCUMENT AVAILABLE



BEST DOCUMENT AVAILABLE

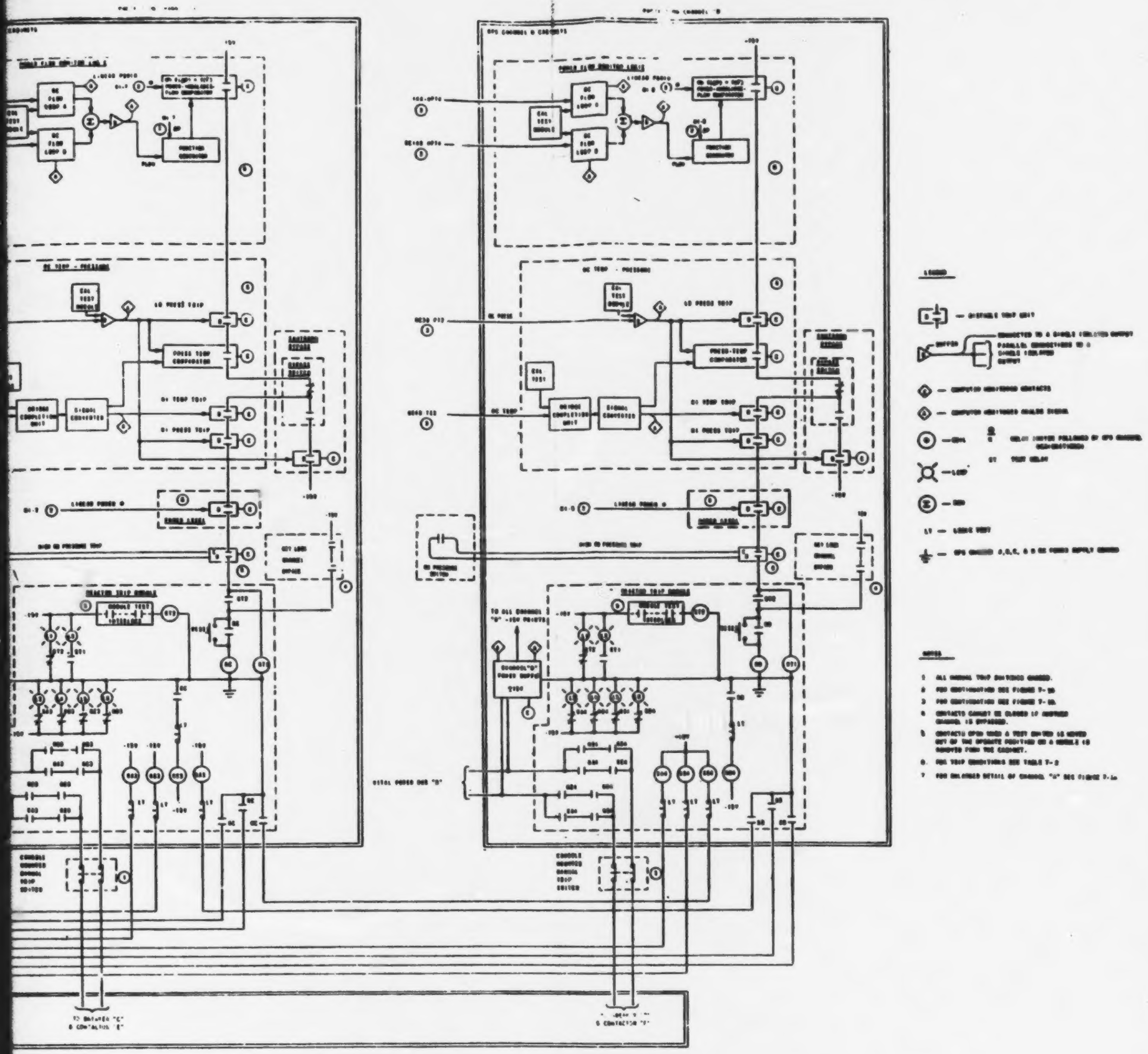


Figure A.1 (1/2) Reactor Protection System Schematic Diagram

19-A

[redacted]

BEST DOCUMENT AVAILABLE

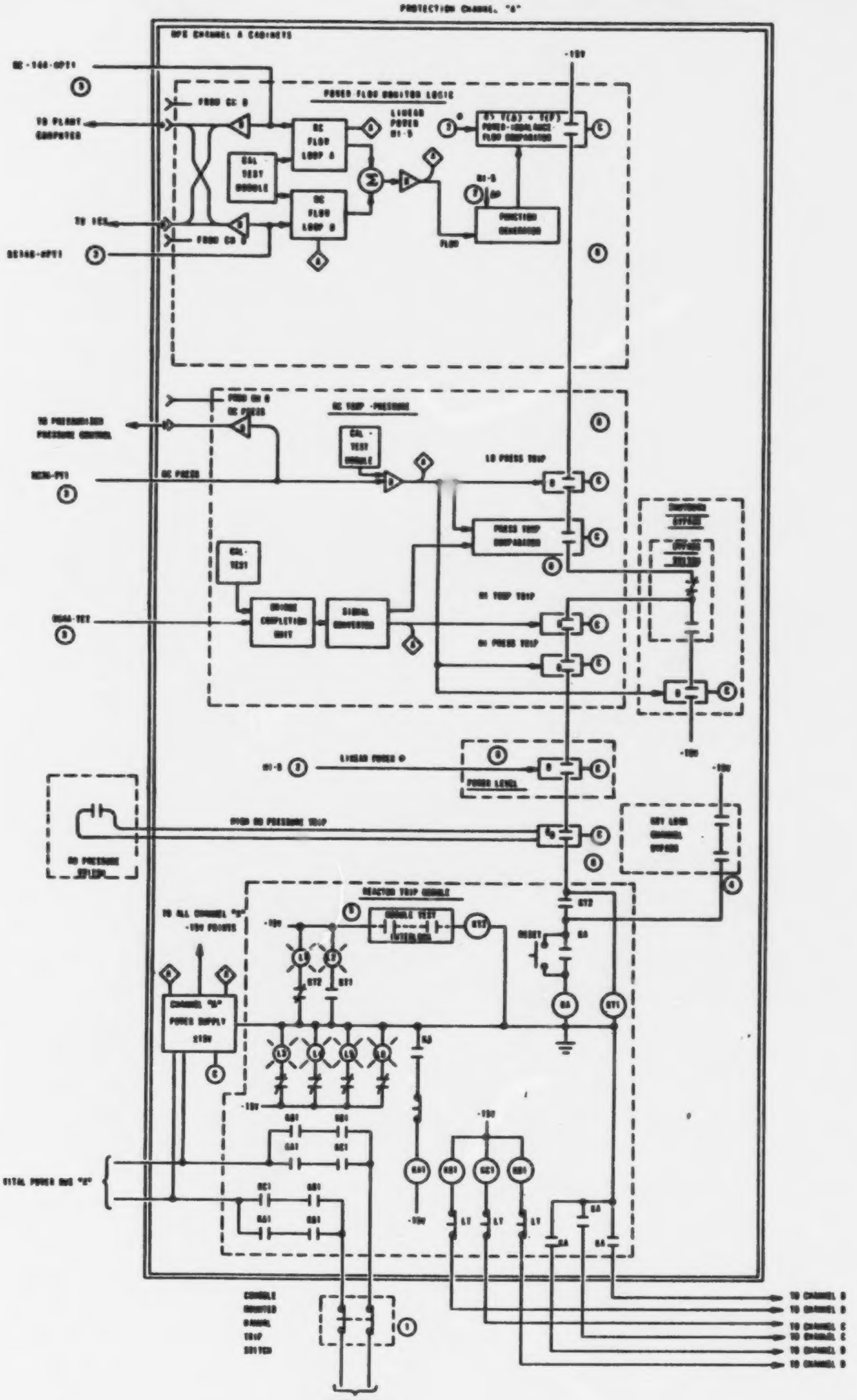
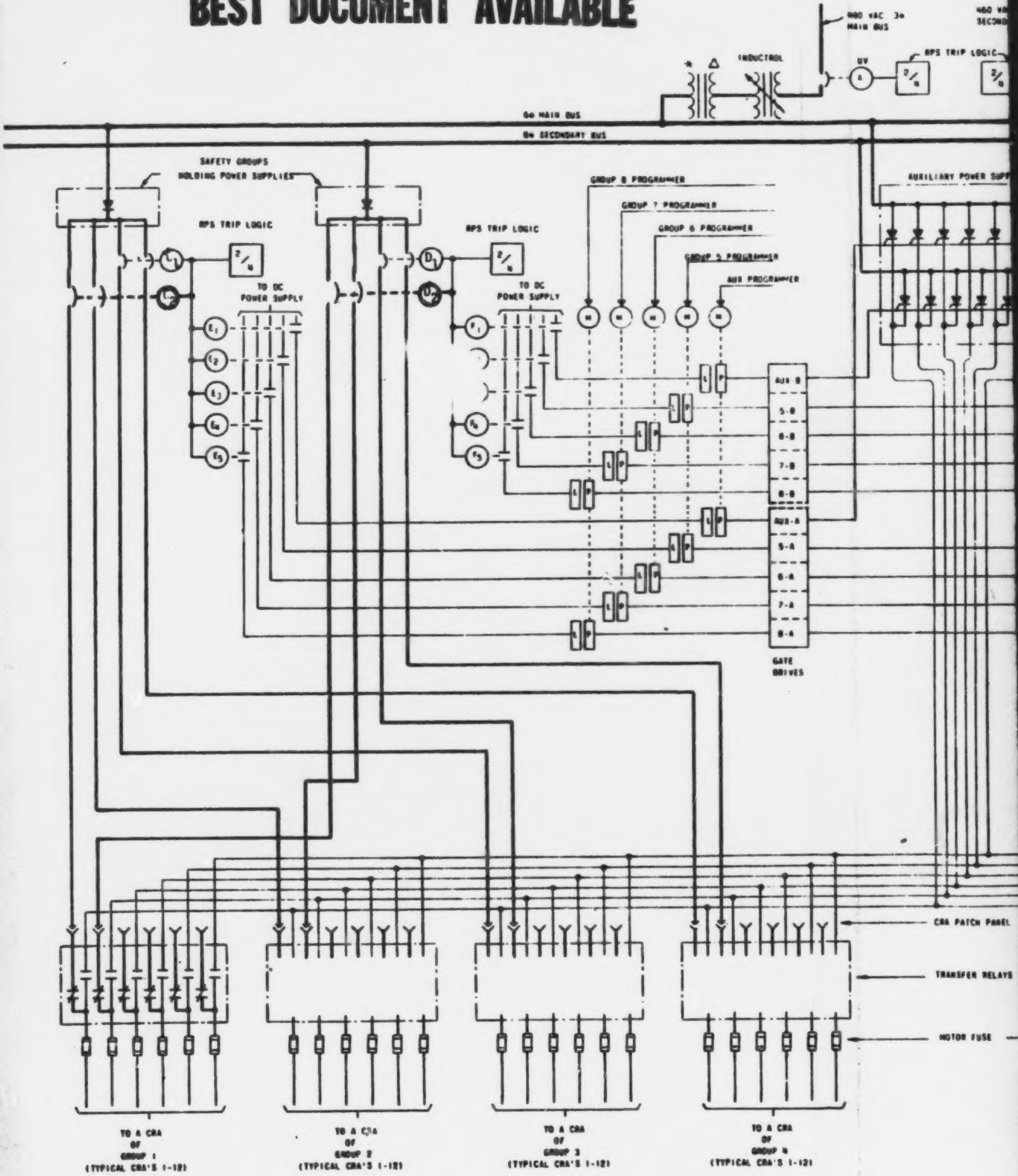

PROTECTION CHANNEL "A"
RPS CHANNEL A CABINETS
-15V
TO PLANT COMPUTER
FROM CC B
POWER FLOW MONITOR LOGIC
RC FLOW LOOP A
RC FLOW LOOP B
CAL TEST MODULE
LINEAR POWER NI-5
POWER-IMBALANCE-FLOW COMPARATOR
FUNCTION GENERATOR
FLOW
TO ICS
RC TEMP - PRESSURE
TO PRESSURIZER PRESSURE CONTROL
RC PRESS
LO PRESS TRIP
PRESS TEMP COMPARATOR
CAL TEST
BRIDGE COMPLETION UNIT
SIGNAL CONVERTER
HI TEMP TRIP
HI PRESS TRIP
SHUTDOWN BYPASS
BYPASS RELAY
NI-5
LINEAR POWER Φ
POWER LEVEL
HIGH RB PRESSURE TRIP
RB PRESSURE SWITCH
KEY LOCK CHANNEL BYPASS
REACTOR TRIP MODULE
TO ALL CHANNEL "A" -15V POINTS
MODULE TEST INTERLOCK
RESET
CHANNEL "A" POWER SUPPLY ±15V
VITAL POWER BUS "A"
CONSOLE MOUNTED MANUAL TRIP SWITCH
TO BREAKER A
TO CHANNEL B
TO CHANNEL C
TO CHANNEL D

Figure A.1 (2/2) Reactor Protection System Schematic Diagram

BEST DOCUMENT AVAILABLE


460 VAC 3φ
MAIN BUS
460 VA
SECOND
INDUCTROL
UV
RPS TRIP LOGIC
2/4
6φ MAIN BUS
6φ SECONDARY BUS
SAFETY GROUPS
HOLDING POWER SUPPLIES
RPS TRIP LOGIC
RPS TRIP LOGIC
TO DC
POWER SUPPLY
TO DC
POWER SUPPLY
D1
D2
E1
E2
E3
E4
E5
F1
F4
F5
GROUP 8 PROGRAMMER
GROUP 7 PROGRAMMER
GROUP 6 PROGRAMMER
GROUP 5 PROGRAMMER
AUX PROGRAMMER
AUXILIARY POWER SUPP
M
L
P
AUX B
5-B
6-B
7-B
8-B
AUX-A
5-A
6-A
7-A
8-A
GATE
DRIVES
CRA PATCH PANEL
TRANSFER RELAYS
MOTOR FUSE
TO A CRA
OF
GROUP 1
(TYPICAL CRA'S 1-12)
TO A CRA
OF
GROUP 2
(TYPICAL CRA'S 1-12)
TO A CRA
OF
GROUP 3
(TYPICAL CRA'S 1-12)
TO A CRA
OF
GROUP 4
(TYPICAL CRA'S 1-12)

BEST DOCUMENT AVAILABLE

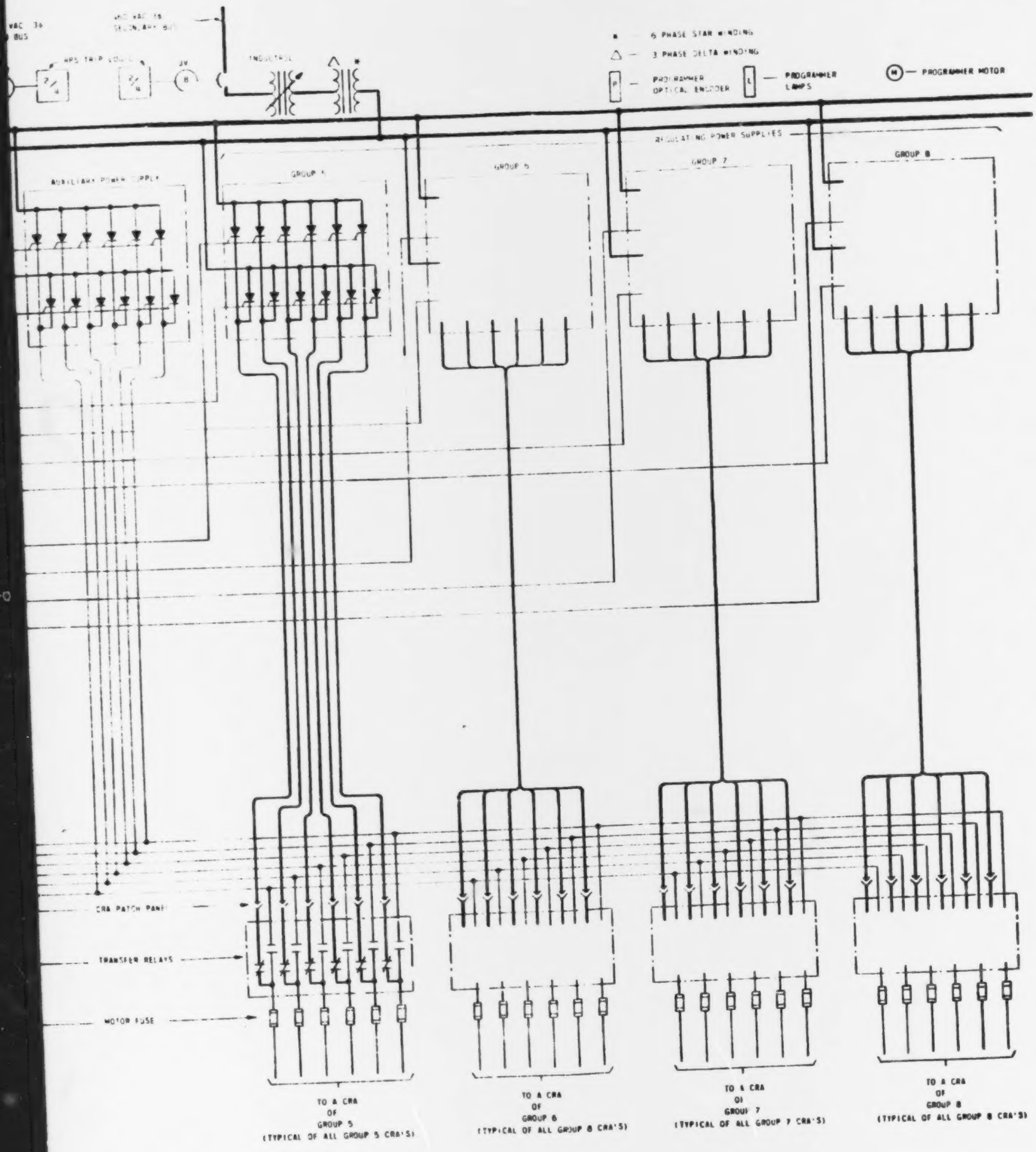

VAC 3φ
BUS
480 VAC 3φ
SECONDARY BUS
RPS TRIP LOGIC
2/4
2/4
3φ
M
INDUCTROL
△
*
* — 6 PHASE STAR WINDING
△ — 3 PHASE DELTA WINDING
P — PROGRAMMER OPTICAL ENCODER
L — PROGRAMMER LAMPS
M — PROGRAMMER MOTOR
REGULATING POWER SUPPLIES
AUXILIARY POWER SUPPLY
GROUP 5
GROUP 6
GROUP 7
GROUP 8
CRA PATCH PANEL
TRANSFER RELAYS
MOTOR FUSE
TO A CRA
OF
GROUP 5
(TYPICAL OF ALL GROUP 5 CRA'S)
TO A CRA
OF
GROUP 6
(TYPICAL OF ALL GROUP 6 CRA'S)
TO A CRA
OF
GROUP 7
(TYPICAL OF ALL GROUP 7 CRA'S)
TO A CRA
OF
GROUP 8
(TYPICAL OF ALL GROUP 8 CRA'S)

Figure A.2 Rod Drive Control System Schematic Diagram

[redacted]

A.2 SYSTEM SIMPLIFIED FAULT TREE

A detailed fault tree for the RPS was constructed, identifying the events which contribute to the failure to insert the control and safety rods into the core when required by reactor conditions.

Failure to automatically remove power to all of the safety and control rods constituted RPS failure. In addition, such faults as core disruption, which would inhibit rod insertion, or stuck rods were included as contributors to reactor trip failures.

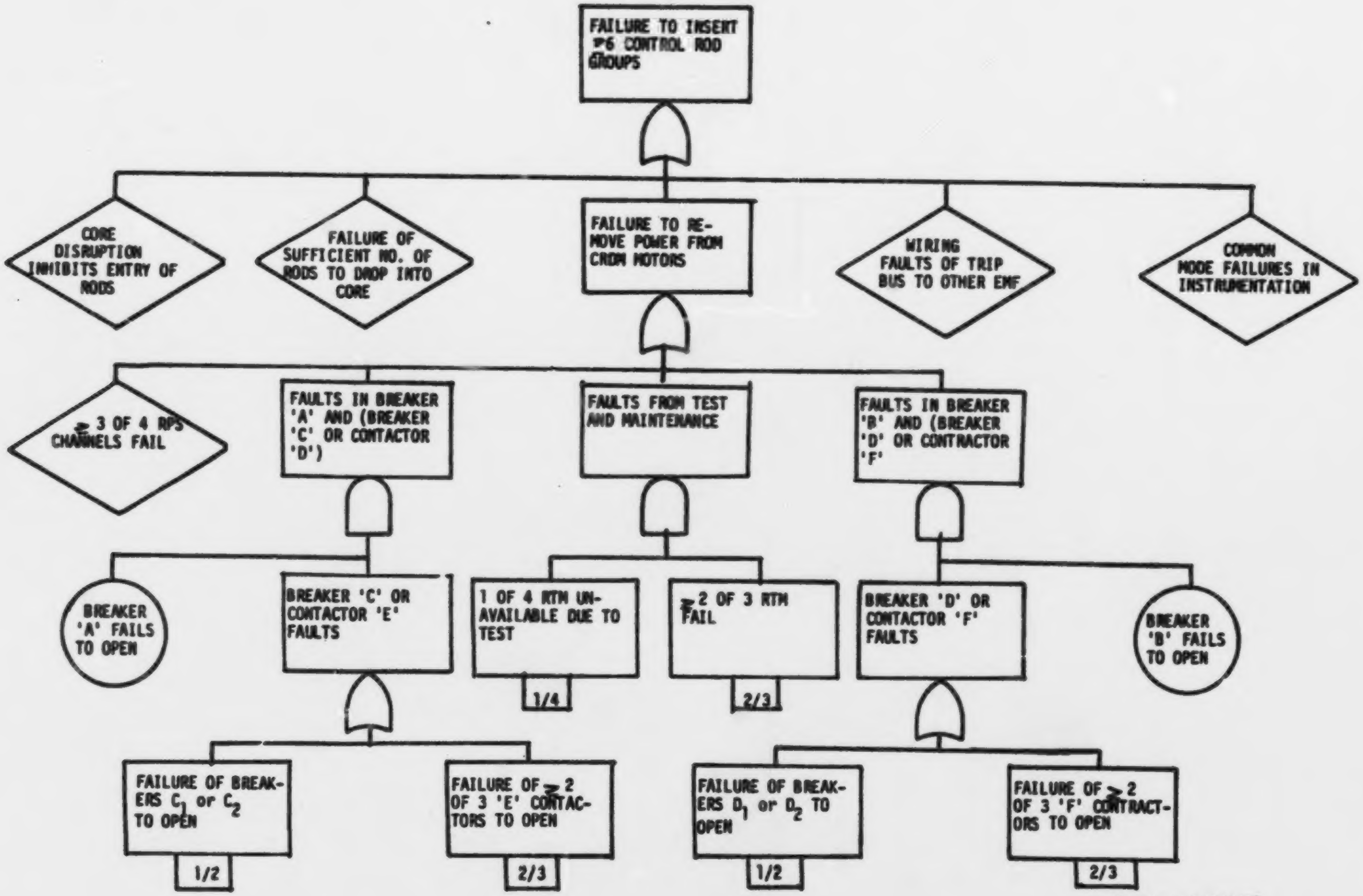
The top event of the fault tree is defined as:

"FAILURE TO INSERT SIX OR MORE CONTROL ROD GROUPS"

The simplified fault tree is shown in Figure A.3.

[redacted]

BEST DOCUMENT AVAILABLE


FAILURE TO INSERT ≥6 CONTROL ROD GROUPS
CORE DISRUPTION INHIBITS ENTRY OF RODS
FAILURE OF SUFFICIENT NO. OF RODS TO DROP INTO CORE
FAILURE TO REMOVE POWER FROM CRDM MOTORS
WIRING FAULTS OF TRIP BUS TO OTHER EMF
COMMON MODE FAILURES IN INSTRUMENTATION
≥ 3 OF 4 RPS CHANNELS FAIL
FAULTS IN BREAKER 'A' AND (BREAKER 'C' OR CONTACTOR 'D')
FAULTS FROM TEST AND MAINTENANCE
FAULTS IN BREAKER 'B' AND (BREAKER 'D' OR CONTRACTOR 'F'
BREAKER 'A' FAILS TO OPEN
BREAKER 'C' OR CONTACTOR 'E' FAULTS
1 OF 4 RTM UNAVAILABLE DUE TO TEST
1/4
≥2 OF 3 RTM FAIL
2/3
BREAKER 'D' OR CONTACTOR 'F' FAULTS
BREAKER 'B' FAILS TO OPEN
FAILURE OF BREAKERS C1 or C2 TO OPEN
1/2
FAILURE OF ≥ 2 OF 3 'E' CONTACTORS TO OPEN
2/3
FAILURE OF BREAKERS D1 or D2 TO OPEN
1/2
FAILURE OF ≥ 2 OF 3 'F' CONTRACTORS TO OPEN
2/3

(Revised 6/19/81)

Figure A.3 Simplified Fault Tree - Reactor Protection System

A.3 SYSTEM QUANTIFICATION

A.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The RPS consists of eight groups of control rods, of which seven groups comprise the emergency safety system. Insertion of six of the seven emergency safety system groups is required for success. Thus, from the standpoint of failures that would fail individual groups, the system is configured in two-out-of-seven redundancy. Failures of this type were assessed to not contribute to RPS unavailability.

The dominant contribution to RPS unavailability was assessed to be due to test of the reactor trip modules (RTM). Faults in the CRD power train primary (AC) breakers and secondary (DC)breakers makeup approximately 35% of the total unavailability. All other contributors are negligible.

A.3.2 SYSTEM FAULT TREE QUANTIFICATION

The Reactor Protection System does not interact with any other system. The independence from any other system does not require a Boolean reduction in the event tree sequence analysis. Therefore, no modularized fault tree was constructed. The simplified fault tree in Figure A.3 was used in slightly modified form for quantification purposes. The modified tree is shown in Figure A.4.

Table A.2 shows the RPS success requirements. Table A.3 contains the top event definitions for the simplified fault tree. The unavailability of each gate is shown on the tree, Figure A.4. Table A.4 shows the Boolean equations that represent the fault tree. Table A.5 shows the quantification of each gate by component and failure mode. Table A.6 summarizes the point estimates and error factors for each gate.

Table A.2 Reactor Protection System

SUCCESS REQUIREMENTS

INITIATOR	TRAINS	NOTES
B_4, Transients	Failure to automatically or manually insert at least six control rod groups.	
B_1, B_2, B_3	None	1

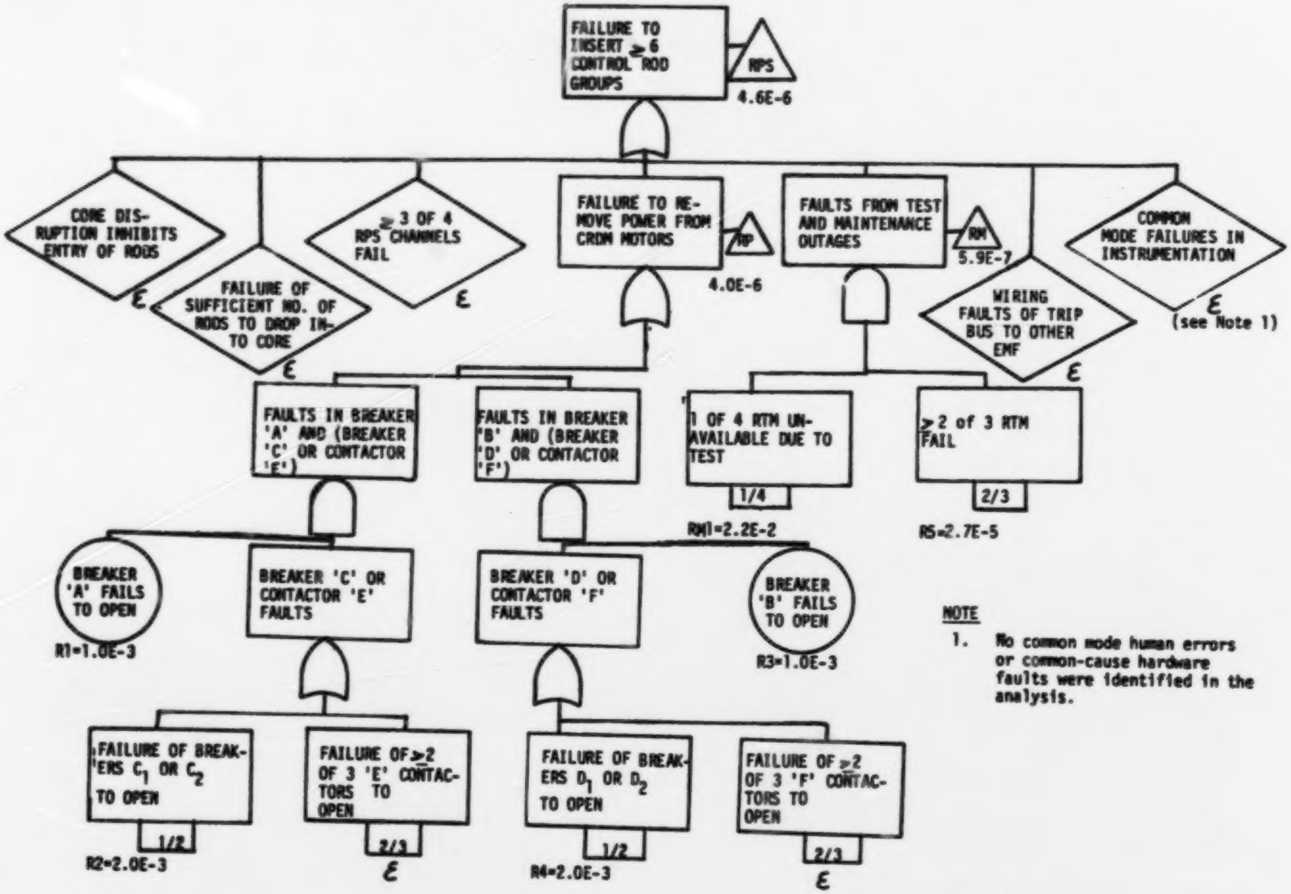
NOTES: 1 For B_1, B_2, B_3 LOCAs it is assumed that the effects of reactor coolant blowdown (removal of moderator) is sufficient to achieve reactor subcriticality. The reactor vessel will be refilled with borated water of sufficient boron concentration to keep the reactor subcritical.

Table A.3 Reactor Protection System

TOP EVENT DEFINITION

BOOLEAN REPRESENTATION	TOP EVENT	NOTES
RPS	Failure to insert at least six control rod groups	
RP	Failure to remove power from CRDM motors	
RM	Faults from test and maintenance outages	

BEST DOCUMENT AVAILABLE


FAILURE TO INSERT ≥ 6 CONTROL ROD GROUPS
RPS
4.6E-6
CORE DISRUPTION INHIBITS ENTRY OF RODS
ε
FAILURE OF SUFFICIENT NO. OF RODS TO DROP INTO CORE
ε
≥ 3 OF 4 RPS CHANNELS FAIL
ε
FAILURE TO REMOVE POWER FROM CRDM MOTORS
RP
4.0E-6
FAULTS FROM TEST AND MAINTENANCE OUTAGES
RM
5.9E-7
WIRING FAULTS OF TRIP BUS TO OTHER EMF
ε
COMMON MODE FAILURES IN INSTRUMENTATION
ε
(see Note 1)
FAULTS IN BREAKER 'A' AND (BREAKER 'C' OR CONTACTOR 'E')
FAULTS IN BREAKER 'B' AND (BREAKER 'D' OR CONTACTOR 'F')
1 OF 4 RTM UNAVAILABLE DUE TO TEST
1/4
RM1=2.2E-2
≥ 2 of 3 RTM FAIL
2/3
R5=2.7E-5
BREAKER 'A' FAILS TO OPEN
R1=1.0E-3
BREAKER 'C' OR CONTACTOR 'E' FAULTS
BREAKER 'D' OR CONTACTOR 'F' FAULTS
BREAKER 'B' FAILS TO OPEN
R3=1.0E-3
FAILURE OF BREAKERS C1 OR C2 TO OPEN
1/2
R2=2.0E-3
FAILURE OF ≥2 OF 3 'E' CONTACTORS TO OPEN
2/3
ε
FAILURE OF BREAKERS D1 OR D2 TO OPEN
1/2
R4=2.0E-3
FAILURE OF ≥2 OF 3 'F' CONTACTORS TO OPEN
2/3
ε

NOTE

1. No common mode human errors or common-cause hardware faults were identified in the analysis.

(Rev. 6/19/81)

Figure A.4 Simplified Fault Tree (Modified) - Event "RPS"

Table A.4 Reactor Protection System

BOOLEAN EQUATIONS BASED ON SIMPLIFIED FAULT TREE

TOP EVENT	NOTES
$RPS = RP + RM$	(1)
$RP = R1 \cdot R2 + R3 \cdot R4$	
$RM = RM1 \cdot R5$	

NOTES: 1. All basic events that are assessed to be negligible contributors (ε) were not included in the Boolean equation.

Table A.5 Events "RP" and "RM" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
RP		FAILURE (HARDWARE) TO REMOVE POWER FROM CRDM MOTORS			4.0 E-6			
R1	BREAKER	FAILS TO OPEN	D		1.0 E-3	$3^+,3^-$		
R2	BREAKERS "C"	FAIL TO OPEN (1/2)	D		2.0 E-3 ϒ=2.0 E-6	$3^+,3^-$		
R3	BREAKER "B"	FAILS TO OPEN	D		1.0 E-3	$3^+,3^-$		
R4	BREAKERS "D"	FAIL TO OPEN (1/2)	D		2.0 E-3 ϒ=2.0 E-6	$3^+,3^-$		
					Σ=4.0 E-6			
RM		TEST AND MAINTENANCE RELATED FAULTS			5.9 E-7			
RM1	RTM	UNAVAILABLE DUE TO TEST (1/4)			2.2 E-2		1	
R5	RTM	≥2 OF 3 RTM FAIL (2/3)			2.7 E-5 ϒ=5.9 E-7	$3^+,3^-$	2	

Table A.5 Reactor Protection System

QUANTIFICATION TABLES

NOTES

1 . Each of the four reactor trip modules (RTM) is assumed to be unavailable for an average of four hours per month due to test. The total test outage for the RTM channels is thus 16 hours and the total unavailability from these tests is (16)/(720) = 2.2 E-2.

2 Failure of (2/3) RTMs was assessed to be 2.7 E-5. The individual RTM failure probability was assessed at 3.0 E-3 rather than the more normal assessment of 1.0 E-2 due to the simplification of the calibration procedure which results from the built-in test and calibration circuits in the equipment. The multiple failures of the RTM were assumed to be independent due to staggered test and calibration, thus the total unavailability of (2/3) RTMs is $3(3.0\ E\text{-}3)^2 = 2.7\ E\text{-}5$.

Table A.6 RPS - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES'
R1	1.0 E-3
R2	2.0 E-3
R3	1.0 E-3
R4	2.0 E-3
R5	2.7 E-5
RM1	2.2 E-2

APPENDIX B

ENGINEERED SAFEGUARDS ACTUATION SYSTEM

APPENDIX B ENGINEERED SAFEGUARDS ACTUATION SYSTEM (ESAS)

B.1 SYSTEM DESCRIPTION AND OPERATION

The Engineered Safeguard Actuation System (ESAS) monitors two variables -- reactor coolant pressure and reactor building pressure -- to detect loss of coolant system boundary integrity. Upon detection of "out-of-limit" conditions of these variables, it initiates operation of the high pressure injection (HPI), low pressure injection (LPI), reactor building isolation and cooling (RBIC), and reactor building spray system (RBSS). The ESAS also starts the engineered safeguards diesel generators A and B.

B.1.1 SYSTEM DESCRIPTION

The ESAS consists of two separate redundant actuation subsystems (trains) A and B, each of which is dedicated to a corresponding ES equipment train. Each ESAS train consists of three sets of channel cabinets, an actuation relay cabinet and the appropriate section of the engineered safeguard operating panel. The equipment in each of the channel cabinets is comprised of the bistable trip units, bistable auxiliary relays, bypass relays, test relays, relay status lights and test switches.

The actuation relay cabinet is divided into four separate compartments to contain the relays for each actuation subsystem and manual actuation output relays. Each of the output signals from a train (the actuation signals for the equipment) is generated by combining the inputs from the three channels in a two out of three matrix as shown in the simplified ESAS logic diagram presented in Figure B.1. Each ESAS train generates five types of output signals: RBSS, RBIC, LPI, HPI and the diesel generator emergency loading sequence, which is provided for sequential starting of large electrical loads following detection of an "out-of-limit" condition.

The following is a simplified description of system operation of train A (or B):

Each actuation train employs three logic channels and the outputs of these channels are used in two-out-of-three coincidence networks for equipment actuation. The channels are actuated by receiving signals (information) from the various on-going processes within the reactor plant and containment. The signal actuates the channel logic by de-energizing to trip the instrumentation channel output relays by opening the contacts, e.g., relay R3 (these output relays are normally energized with closed contacts). See Figure B.2.

Similarly, the logic matrices (actuation relays) in the actuation channels are de-energized to trip -- contacts close, e.g., relay Z1A -- and actuate the engineered safeguards equipment. (The actuation relays are normally energized with contacts open).

Separate essential service and DC power supplies are used for each actuation channel.

The following paragraphs contain a discussion of the specific relay logic implementation used in the actuation channels of each of the five types of ESAS actuation signals.

HIGH PRESSURE INJECTION (HPI) AND DIESEL GENERATOR EMERGENCY LOADING SEQUENCE (DGELS)

Referring to one of three independent reactor coolant pressure transmitters shown in Figure B.3, a signal proportional to the reactor coolant pressure is applied to a safeguards bistable (BT1) and to a bypass bistable. The design of safeguard bistables is such that when the reactor coolant pressure is above the setpoint and control power is available, bistable interposing relay R3 is energized.

HPI is initiated by de-energizing the multiple contact output relays constituting loading sequence block 1 in two-out-of-three channels. (Block 1 consists of HP Injection pumps, Injection and Nuclear Services Valves, and LP Injection pumps). The multiple contact output relays can be de-energized by the manual actuation relay by their related test contact, or by an "OR" function made up of contacts which open when the reactor coolant pressure is below 1500 psig (R3), the building pressure exceeds 4 psig (R12), or the reactor coolant pressure is below 500 psig.

Blocks 2, 3, and 4 de-energize through an "AND" function, combining an "OR" function similar to the one described above and undervoltage relay contacts from corresponding 4160 volt safeguard bus. Block 2 consists of Reactor Building Fans and Emergency Nuclear Service Seawater pumps. Block 3 consists of Emergency Nuclear Services Closed Cycle Cooling Water pumps. Block 4 consists of spray pump start permit, reactor building ventilation recirculation unit, Decay Heat Closed Cycle Cooling water pump, and Decay Heat Service Seawater pumps.

LOW PRESSURE INJECTION (LPI)

The channels of low pressure injection are equipped with bistables similar to those used for HPI but which are adjusted to actuate at a lower setpoint. A typical channel is shown in Figure B.3. The output of the bistables will de-energize the same output relay as the HPI bistables at 500 psig.

The bypass enabling contact of the bistable closes when the reactor coolant pressure is below its setpoint (900 psig) and control power is available. This action permits manual bypass of the channel for normal shutdown of the system.

REACTOR BUILDING ISOLATION AND COOLING (RBIC)

The channels of Reactor Building Isolation and Cooling are similar in design to the channels of HPI and loading sequence except for the bistable and bypass circuit, as shown in Figure B.4. When the reactor building pressure is below 4 psig and control power is available, pressure switch interposing relay R10 is energized to the reset state by means of the bypass reset pushbutton. A subsequent loss of power or rise in building pressure above setpoint will drop out R10.

The continuous bypass of a channel is possible only after a two-out-of-three actuation. De-energizing the output relays of two-out-of-three channels initates reactor building isolation, starts reactor building emergency cooling and opens all valves required for reactor building spray. The reactor building pressure is sensed by two sets of three pressure switches, and the bypass can only be energized after a two-out-of-three actuation.

REACTOR BUILDING SPRAY (RBSS)

RBSS is initiated by starting the pumps when reactor building pressure is over 30 psig. This is achieved, as shown on Figure B.5, by sensing the reactor building pressure with two sets of three pressure switches. Each set of three pressure switches, which are wired in a two-out-of-three matrix, controls the closing coils of the circuit breaker of one spray pump along with actuation of the spray pump start permit matrix from HPI.

While independence between individual channels within ESAS actuation trains is realized, a dependency exists between actuation trains which include reactor coolant pressure trip signals (HPI, DGELS, LPI, and RBSS). This dependency can be observed by noticing that the channel pressure transducer shown in Figure B.3 provides pressure signals to both LPI and HPI bistables, and that those bistables are common to both actuation trains. Failures of the pressure transducer or bistables affects both actuation trains. Another interface is the undervoltage relay contact appearing in the loading sequence circuitry which represents a dependency on the 4160V ES bus.

The ESAS is not dependent on control power to accomplish equipment actuation since loss of power will de-energize the output relays and activate the associated equipment.

B.1.2 SYSTEM OPERATION

Table B.1 illustrates ESAS equipment actuation signals as a function of reactor coolant pressure and reactor building pressure. Table B.2

lists the trip parameters met, along with ES equipment actuated during various size LOCA events. Loss of power to the ESAS circuitry results in the generation of trip signals by the ESAS (except for RBSS).

The ESAS is designed to allow every component in the system to be tested during plant operation. Typically, monthly surveillance tests are performed to insure all components are operating correctly. System calibration is performed during refueling. The pressure transducers and buffer amplifiers in the system are monitored at shift changes by observing a meter which indicates reactor pressure sensed by the system.

Monthly surveillance tests are performed for the entire system except for the reactor coolant pressure transducers and most of the actuation matrix relay contacts. Each of the ESAS channels is checked individually by generating trip signals. These signals de-energize the output relays of the channel and cause 1 of the 3 relays in the 2 of 3 relay matrices to trip. Equipment will be actuated upon receipt of a trip signal from either of the other 2 channels. Testing of the system does not disable it or reduce its capability to trip. Only one channel can be tested at a time.

During each refueling (every 18 months) tests are done which trigger the ES actuation system one actuation system (train A or B) at a time, then phase into a diesel generator test. These tests are performed using any two (of the three) associated RBIS pressure test switches to introduce an artificial high reactor building pressure signal. These signals de-energize the actuation relays of two out of three channels in the equipment matrices and consequently actuate the equipment.

Table B.1 ESAS Actuation Signals for RCS and RB Pressure Set Points

RCS Pressure Set Point (psig)	ESAS Actuation Description	RB Pressure Set Point (psig)	ESAS Actuation Description
1700	By-pass is enabled	4	Trip - (HPI, LPI pumps, LPI valves, RB isolation) initiated
1500	Trip can be by-passed (HPI, LPI pump)		
1500	Trip HPI, LPI pumps initiated	30	Start containment spray pumps if HPI trip not by-passed
900	Trip can be by-passed (HPI, LPI)		
500	Trip (HPI, LPI pumps, LPI valves) initiated		

Table B.2 ESAS Trip Parameters Met and Systems Actuated for Various Sizes of LOCA Initiating Events

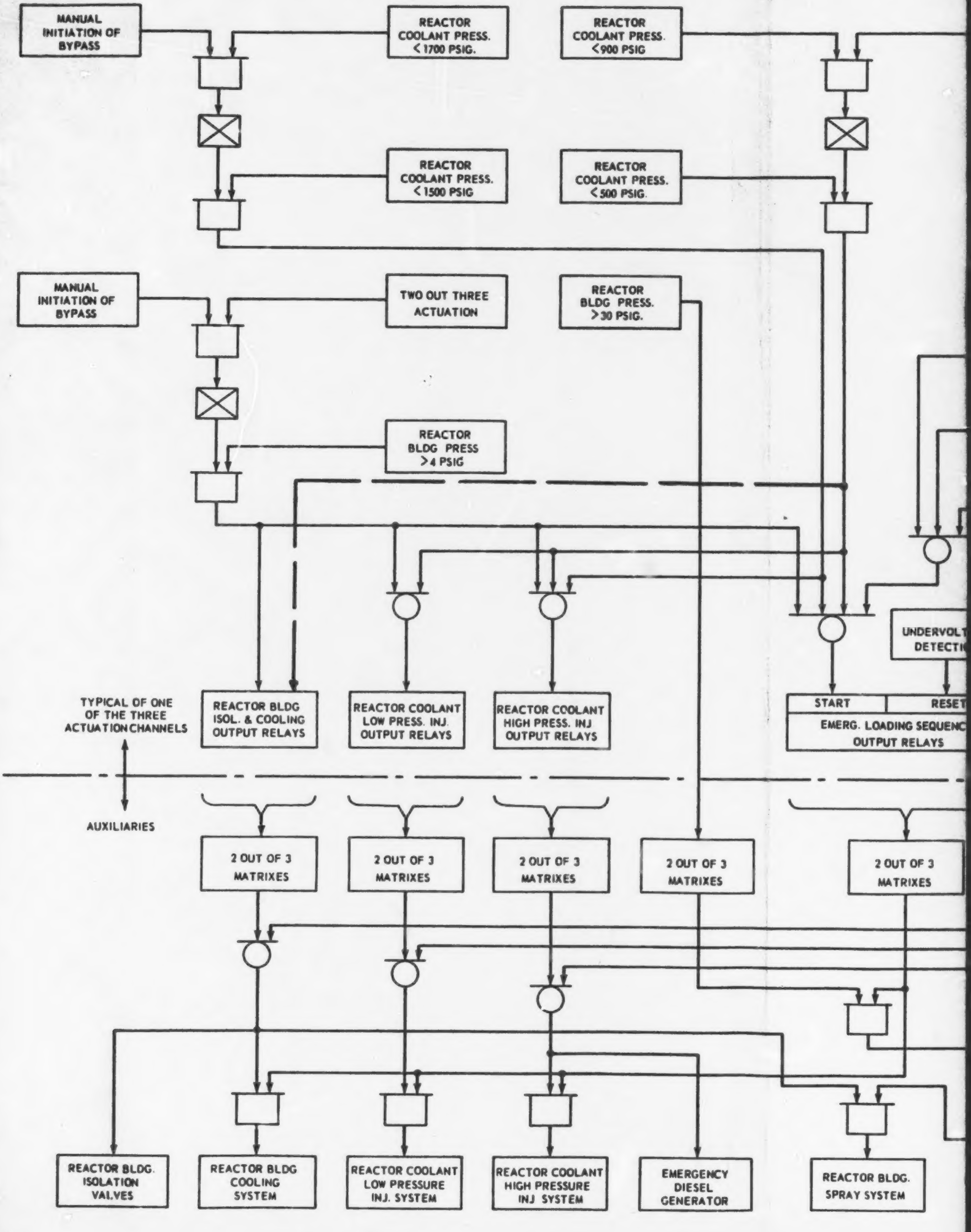
INITIATING EVENTS		TRIP PARAMETERS MET 500 PSI TRIP	 1500 PSI TRIP	 4PSI TRIP	 30PSI TRIP	SYSTEM ACTUATION LPI	 HPI	 RBIC	 RBSS
B_1	Large LOCA	X	X	X	X	X	X	X	X
B_2	Medium LOCA	X	X	X	X‡	X	X	X	X
B_3	Small LOCA		X	X		X	X	X	X*
B_4	Small small LOCA		X			X**	X***		

‡Based on conservative FSAR calculations.

*RBSS spray line injection valves are actuated (opened) by the 4 psi trip signal. The RBSS pumps do not receive an actuation signal.

**LPI pumps start, but the LPI injection valves do not receive an actuation signal.

***Also isolates those RB isolation valves not associated with containment or RCS heat removal.


MANUAL INITIATION OF BYPASS
REACTOR COOLANT PRESS. <1700 PSIG.
REACTOR COOLANT PRESS. <900 PSIG
REACTOR COOLANT PRESS. <1500 PSIG
REACTOR COOLANT PRESS. <500 PSIG.
MANUAL INITIATION OF BYPASS
TWO OUT THREE ACTUATION
REACTOR BLDG PRESS. >30 PSIG.
REACTOR BLDG PRESS >4 PSIG
UNDERVOLT DETECTI
TYPICAL OF ONE OF THE THREE ACTUATION CHANNELS
REACTOR BLDG ISOL. & COOLING OUTPUT RELAYS
REACTOR COOLANT LOW PRESS. INJ. OUTPUT RELAYS
REACTOR COOLANT HIGH PRESS. INJ OUTPUT RELAYS
START
RESET
EMERG. LOADING SEQUENC OUTPUT RELAYS
AUXILIARIES
2 OUT OF 3 MATRIXES
2 OUT OF 3 MATRIXES
2 OUT OF 3 MATRIXES
2 OUT OF 3 MATRIXES
2 OUT OF 3 MATRIXES
REACTOR BLDG. ISOLATION VALVES
REACTOR BLDG COOLING SYSTEM
REACTOR COOLANT LOW PRESSURE INJ. SYSTEM
REACTOR COOLANT HIGH PRESSURE INJ SYSTEM
EMERGENCY DIESEL GENERATOR
REACTOR BLDG. SPRAY SYSTEM

BEST DOCUMENT AVAILABLE

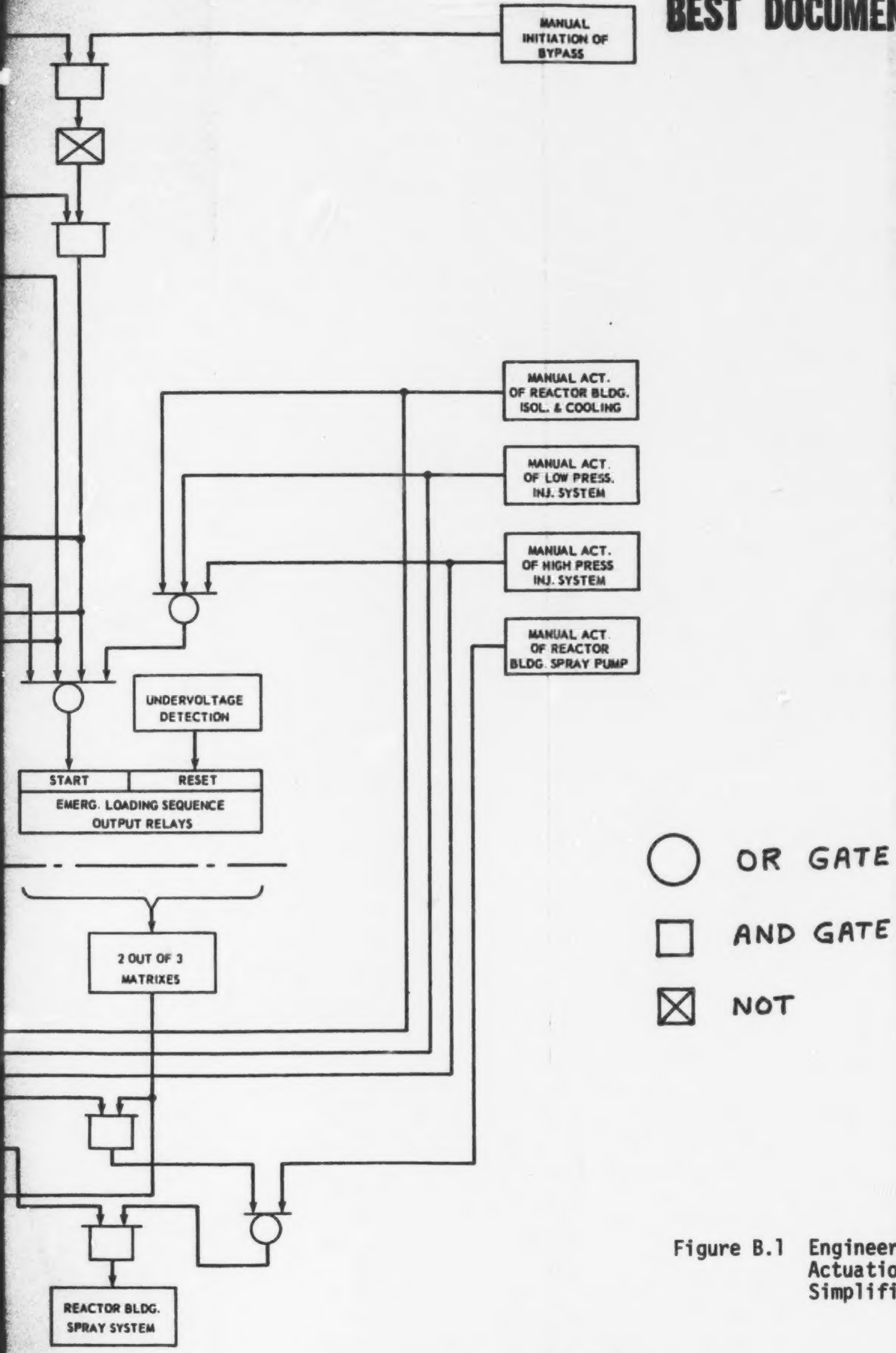
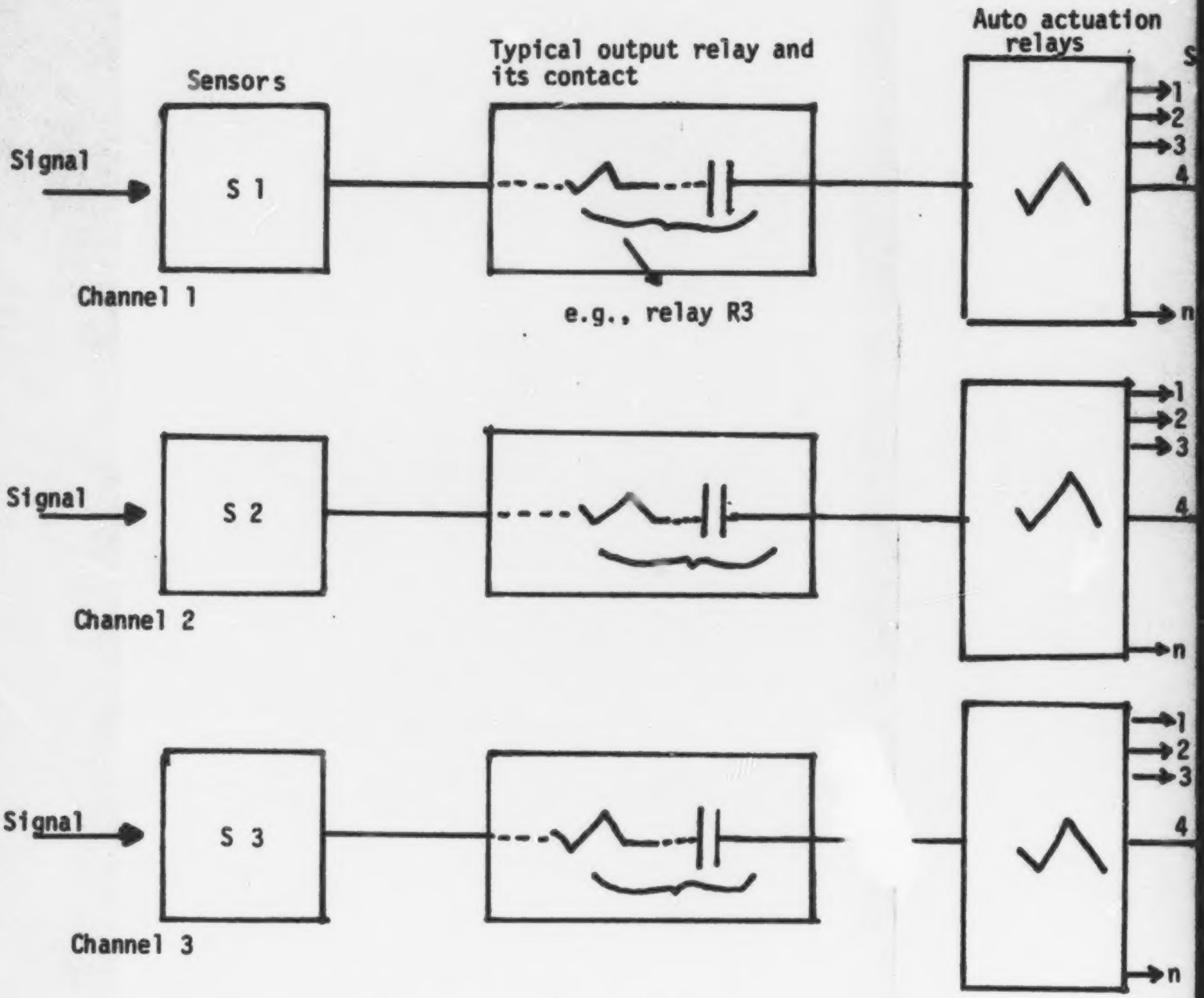

MANUAL INITIATION OF BYPASS
MANUAL ACT. OF REACTOR BLDG. ISOL. & COOLING
MANUAL ACT. OF LOW PRESS. INJ. SYSTEM
MANUAL ACT. OF HIGH PRESS INJ. SYSTEM
MANUAL ACT. OF REACTOR BLDG. SPRAY PUMP
UNDERVOLTAGE DETECTION
START
RESET
EMERG. LOADING SEQUENCE OUTPUT RELAYS
2 OUT OF 3 MATRIXES
REACTOR BLDG. SPRAY SYSTEM
OR GATE
AND GATE
NOT

Figure B.1 Engineered Safeguards Actuation A (B similar) Simplified Logic

BEST DOCUMENT AVAILABLE


Sensors
Typical output relay and its contact
Auto actuation relays
S
Signal
S 1
1
2
3
4
n
Channel 1
e.g., relay R3
Signal
S 2
1
2
3
4
n
Channel 2
Signal
S 3
1
2
3
4
n
Channel 3

The circuits are shown tripped

NOTE 1 Contacts 1, 2, 3, ...n belong to matrixes of other equipment
NOTE 2 Each relay closes two contacts (one U and one Z)

BEST DOCUMENT AVAILABLE

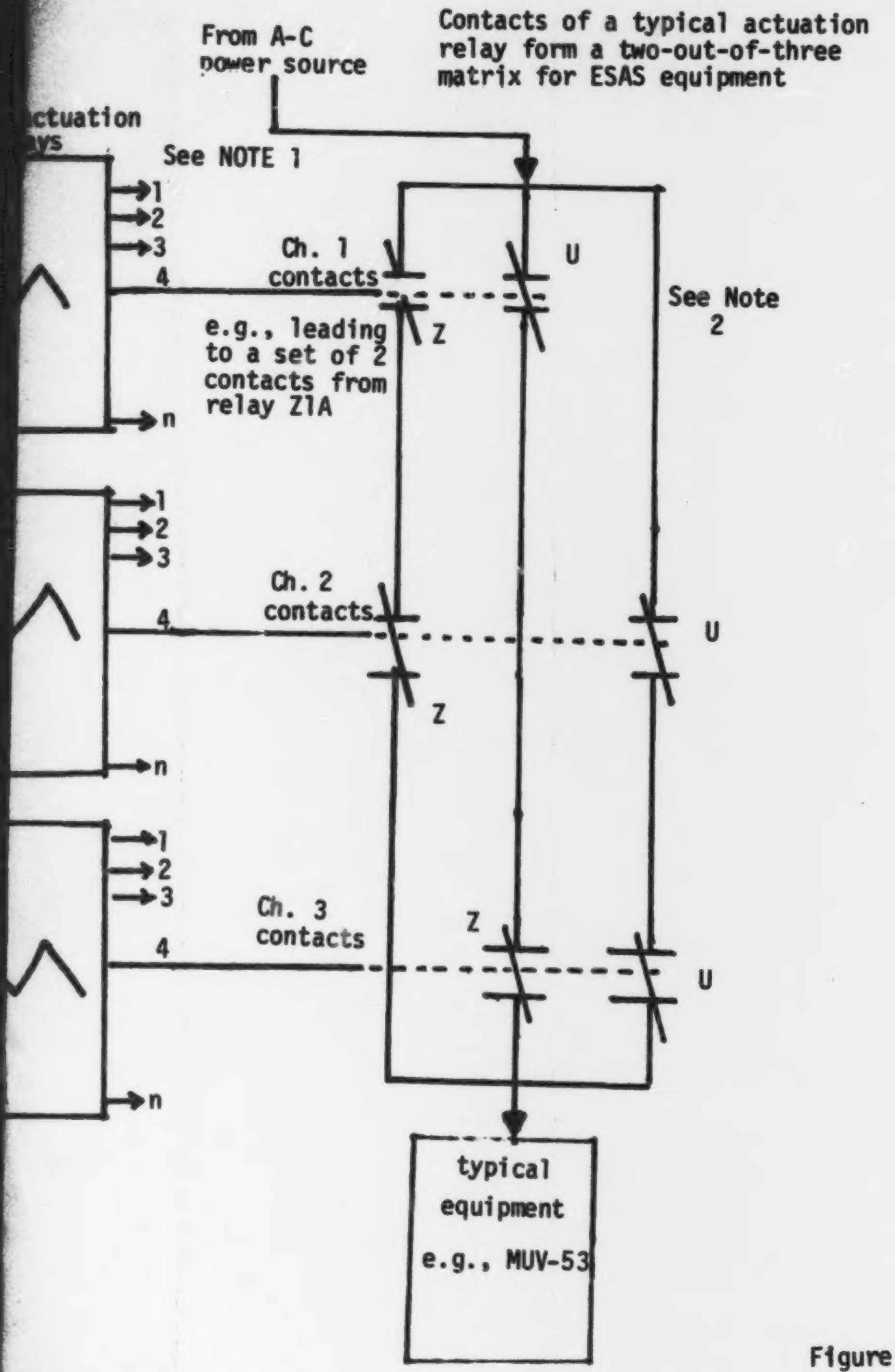
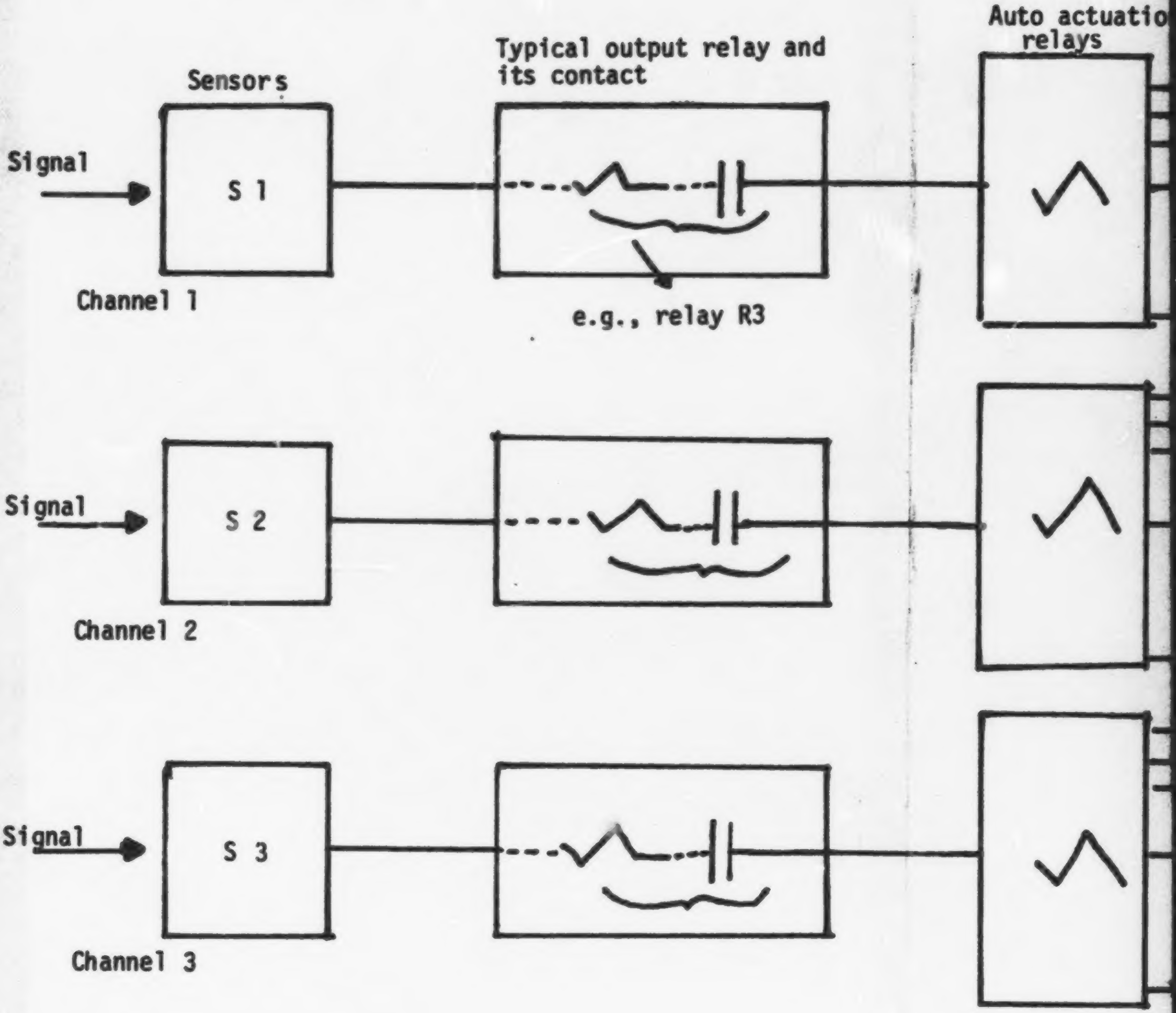

From A-C power source
Contacts of a typical actuation relay form a two-out-of-three matrix for ESAS equipment
ctuation
ys
See NOTE 1
1
2
3
4
n
Ch. 1 contacts
U
Z
See Note 2
e.g., leading to a set of 2 contacts from relay Z1A
1
2
3
4
n
Ch. 2 contacts
Z
U
1
2
3
4
n
Ch. 3 contacts
Z
U
typical equipment
e.g., MUV-53

Figure B.2 ESAS-Simplified Circuitry

[illegible]


Auto actuatio
relays
Typical output relay and
its contact
Sensors
Signal
S 1
Channel 1
e.g., relay R3
Signal
S 2
Channel 2
Signal
S 3
Channel 3

The circuits are shown tripped

NOTE 1 Contacts 1, 2, 3, ...n belong to matrixes of other equipment
NOTE 2 Each relay closes two contacts (one U and one Z)

BEST DOCUMENT AVAILABLE

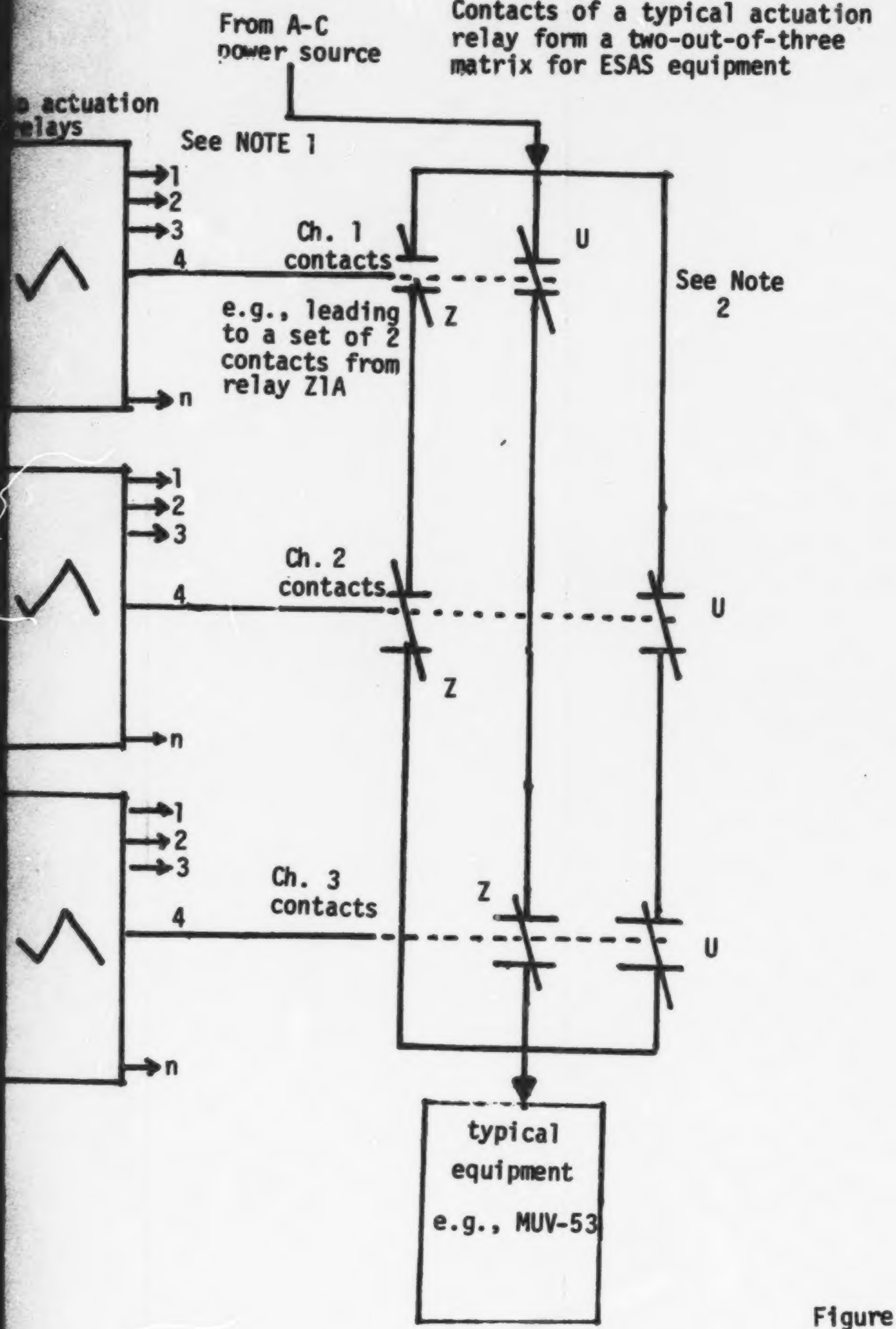
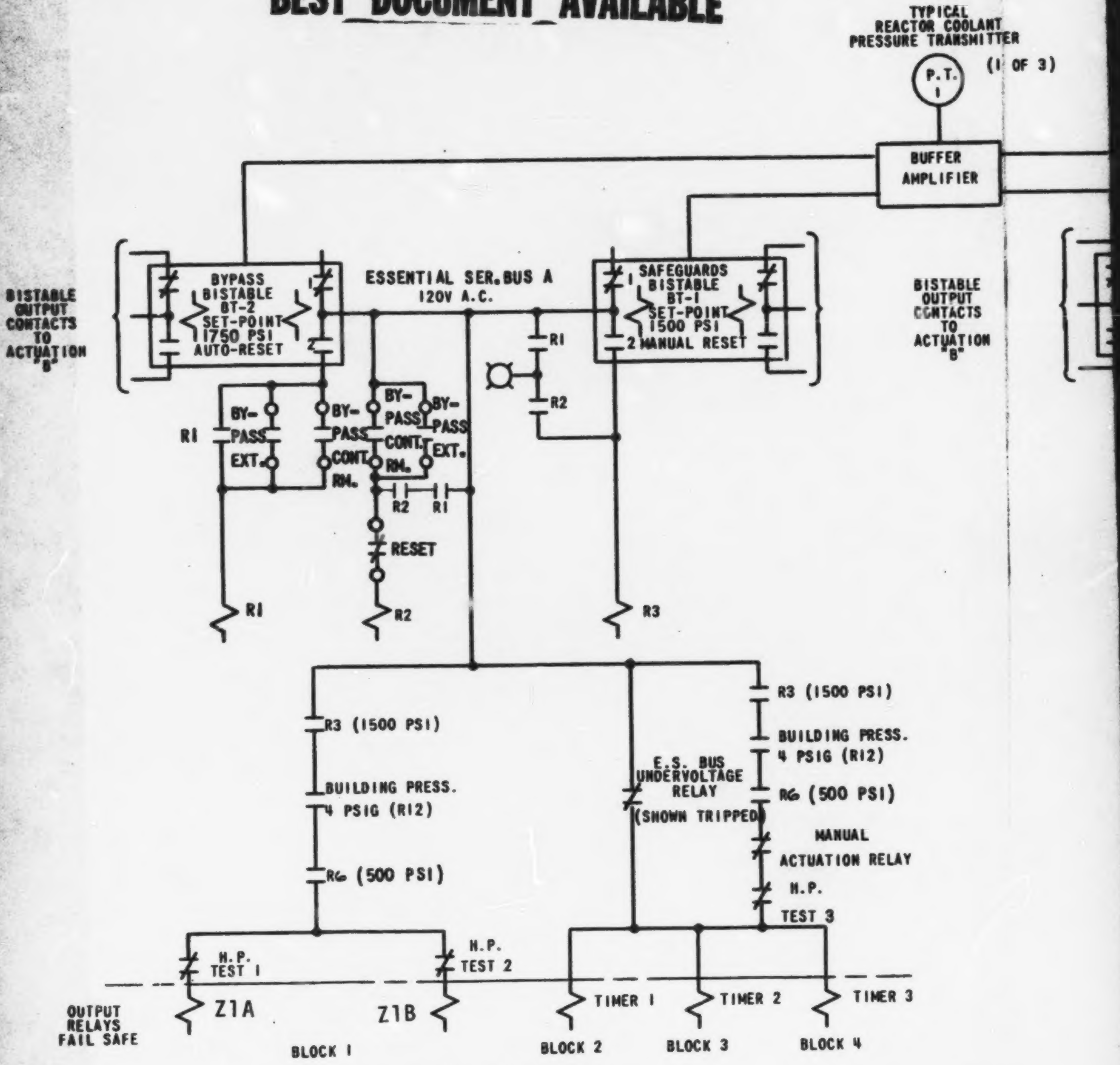

From A-C power source
Contacts of a typical actuation relay form a two-out-of-three matrix for ESAS equipment
actuation
elays
See NOTE 1
1
2
3
4
n
Ch. 1 contacts
U
See Note 2
e.g., leading to a set of 2 contacts from relay Z1A
Z
1
2
3
4
n
Ch. 2 contacts
U
Z
1
2
3
4
n
Ch. 3 contacts
Z
U
typical equipment
e.g., MUV-53

Figure B.2 ESAS-Simplified Circuitry

BEST DOCUMENT AVAILABLE

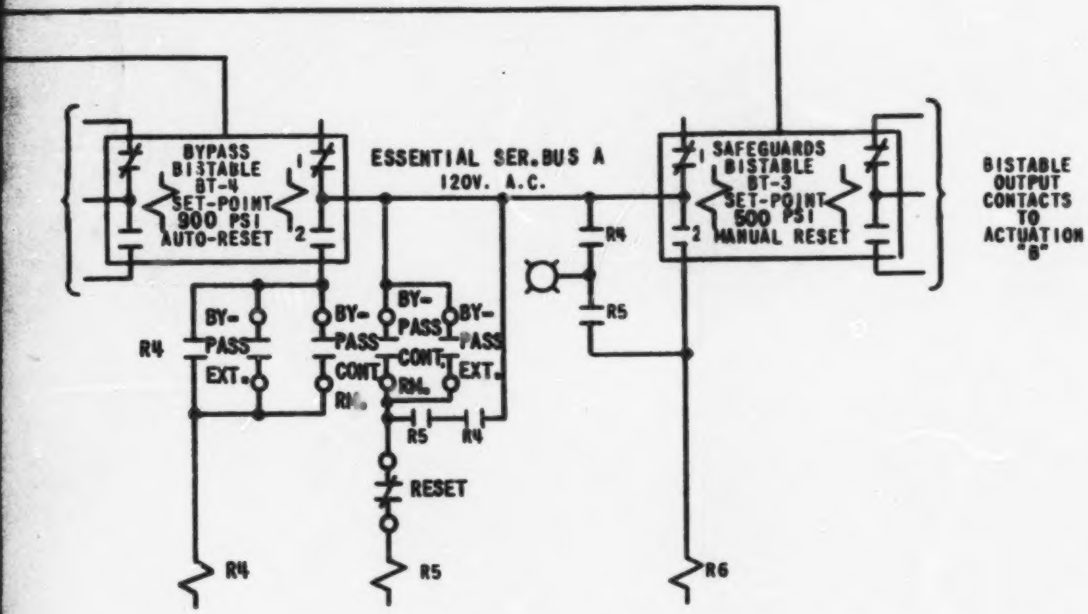

TYPICAL
REACTOR COOLANT
PRESSURE TRANSMITTER
P.T. 1
(1 OF 3)
BUFFER AMPLIFIER
BISTABLE OUTPUT CONTACTS TO ACTUATION "B"
BYPASS BISTABLE BT-2 SET-POINT 1750 PSI AUTO-RESET
1
2
ESSENTIAL SER. BUS A 120V A.C.
SAFEGUARDS BISTABLE BT-1 SET-POINT 1500 PSI MANUAL RESET
1
2
BISTABLE OUTPUT CONTACTS TO ACTUATION "B"
R1
R2
R1
BY-PASS EXT.
BY-PASS CONT. RM.
BY-PASS CONT. RM.
BY-PASS EXT.
R2
R1
RESET
R1
R2
R3
R3 (1500 PSI)
BUILDING PRESS. 4 PSIG (R12)
R6 (500 PSI)
E.S. BUS UNDERVOLTAGE RELAY (SHOWN TRIPPED)
R3 (1500 PSI)
BUILDING PRESS. 4 PSIG (R12)
R6 (500 PSI)
MANUAL ACTUATION RELAY
H.P. TEST 3
H.P. TEST 1
H.P. TEST 2
OUTPUT RELAYS FAIL SAFE
Z1A
Z1B
TIMER 1
TIMER 2
TIMER 3
BLOCK 1
BLOCK 2
BLOCK 3
BLOCK 4

TYPICAL OF 3 CHANNELS
HIGH PRESSURE INJECTION & LOADING SEQUENCE A

NOTE: · 2 OUT OF 3 LOGIC STARTS EAC

BEST DOCUMENT AVAILABLE

F 3)

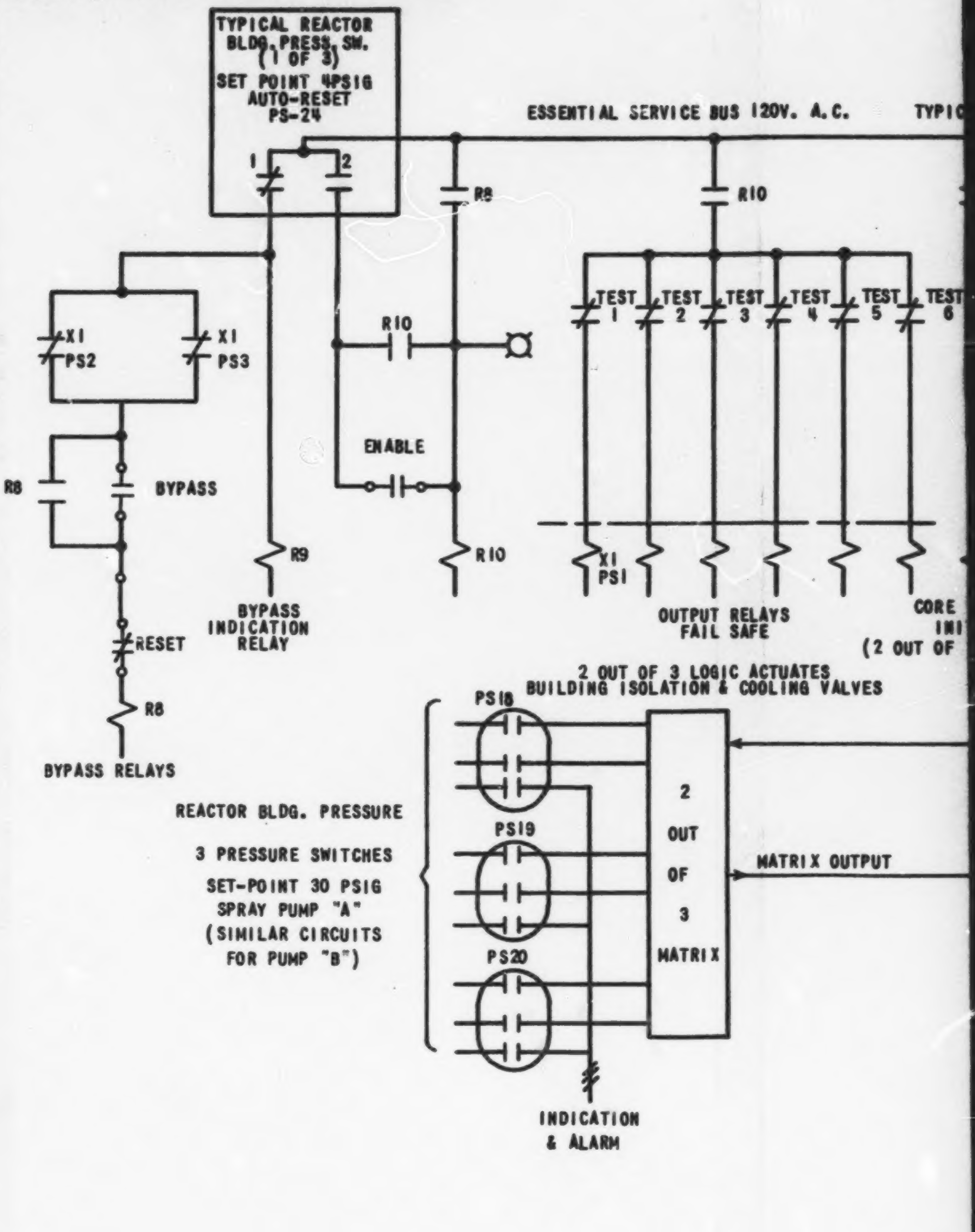

BYPASS
BISTABLE
BT-4
SET-POINT
900 PSI
AUTO-RESET
1
2
ESSENTIAL SER.BUS A
120V. A.C.
SAFEGUARDS
BISTABLE
BT-3
SET-POINT
500 PSI
MANUAL RESET
1
2
BISTABLE
OUTPUT
CONTACTS
TO
ACTUATION
"B"
R4
R5
R4
BY-
PASS
EXT.
BY-
PASS
CONT
RM.
BY-
PASS
CONT.
RM.
BY-
PASS
EXT.
R5
R4
RESET
R4
R5
R6

TYPICAL OF 3 LOW PRESSURE CHANNELS

C STARTS EACH AUXILIARY

Figure B.3 (1/2)
Safeguards Actuation System

BEST DOCUMENT AVAILABLE


TYPICAL REACTOR BLDG. PRESS. SW. (1 OF 3)
SET POINT 4PSIG
AUTO-RESET
PS-24
1
2
ESSENTIAL SERVICE BUS 120V. A.C.
TYPIC
R8
R10
X1
PS2
X1
PS3
R10
ENABLE
R8
BYPASS
RESET
R8
BYPASS RELAYS
R9
BYPASS INDICATION RELAY
R10
TEST 1
TEST 2
TEST 3
TEST 4
TEST 5
TEST 6
X1
PS1
OUTPUT RELAYS FAIL SAFE
CORE
INI
(2 OUT OF
2 OUT OF 3 LOGIC ACTUATES BUILDING ISOLATION & COOLING VALVES
PS18
PS19
PS20
REACTOR BLDG. PRESSURE
3 PRESSURE SWITCHES
SET-POINT 30 PSIG
SPRAY PUMP "A"
(SIMILAR CIRCUITS FOR PUMP "B")
2 OUT OF 3 MATRIX
MATRIX OUTPUT
INDICATION & ALARM

BEST DOCUMENT AVAILABLE

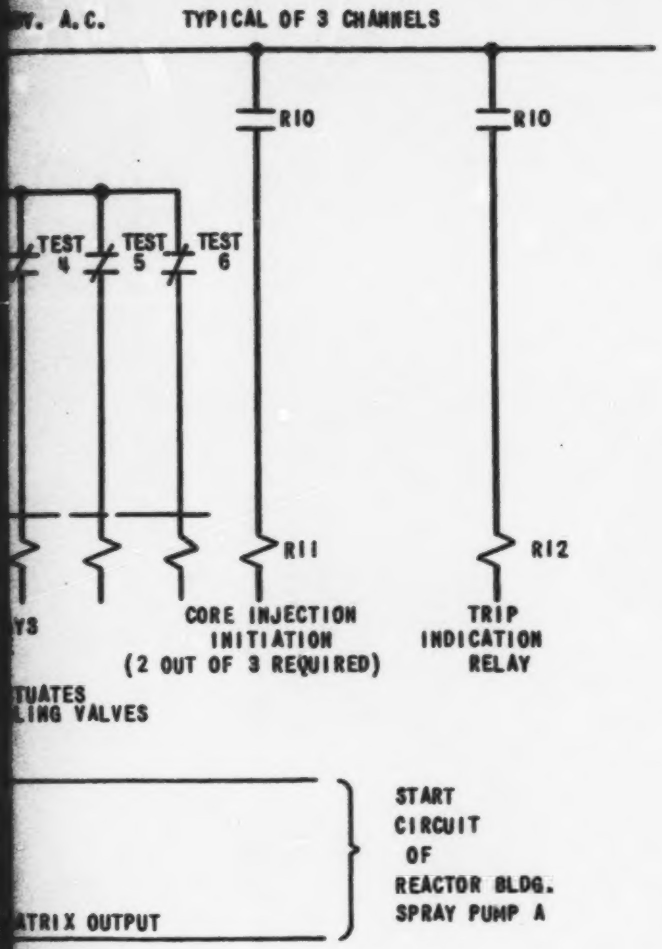

V. A.C.
TYPICAL OF 3 CHANNELS
R10
R10
TEST 4
TEST 5
TEST 6
R11
R12
YS
CORE INJECTION INITIATION (2 OUT OF 3 REQUIRED)
TRIP INDICATION RELAY
TUATES
LING VALVES
START CIRCUIT OF REACTOR BLDG. SPRAY PUMP A
ATRIX OUTPUT

Figure B.3 (2/2)
Safeguards Actuation System

BEST DOCUMENT AVAILABLE

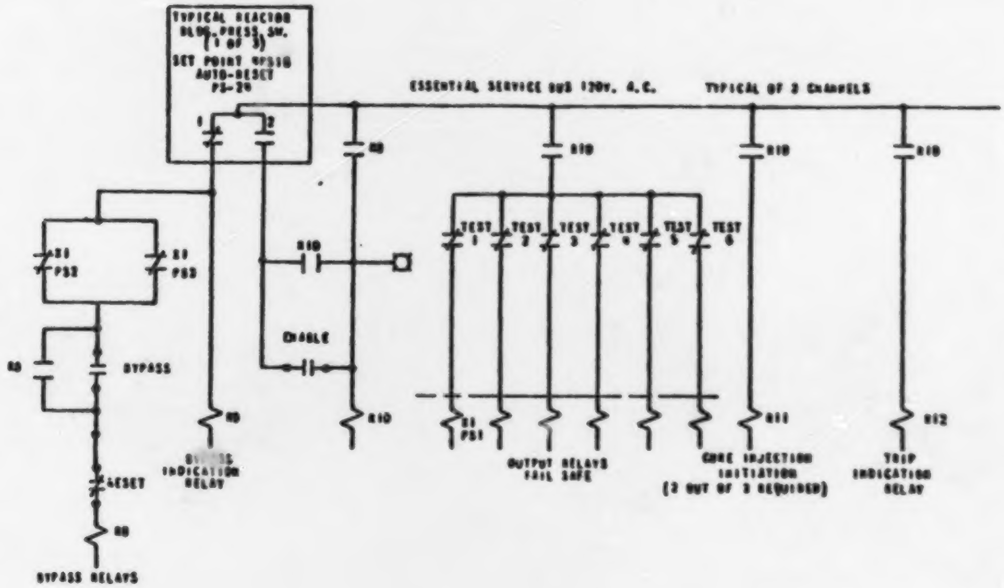

TYPICAL REACTOR BLDG. PRESS. SW. (1 OF 3)
SET POINT 4PSIG
AUTO-RESET
PS-24
1
2
ESSENTIAL SERVICE BUS 120V. A.C.
TYPICAL OF 3 CHANNELS
RB
R10
R10
R10
R10
R1 PS2
R1 PS3
R10
ENABLE
RB
BYPASS
RB
R10
TEST 1
TEST 2
TEST 3
TEST 4
TEST 5
TEST 6
R1 PS1
R11
R12
BYPASS INDICATION RELAY
OUTPUT RELAYS FAIL SAFE
CORE INJECTION INITIATION (2 OUT OF 3 REQUIRED)
TRIP INDICATION RELAY
RESET
RB
BYPASS RELAYS

Figure B.4 Reactor Building Isolation (RBIS) and Cooling (RBCS) Actuation Circuit (1 channel of 1 train)

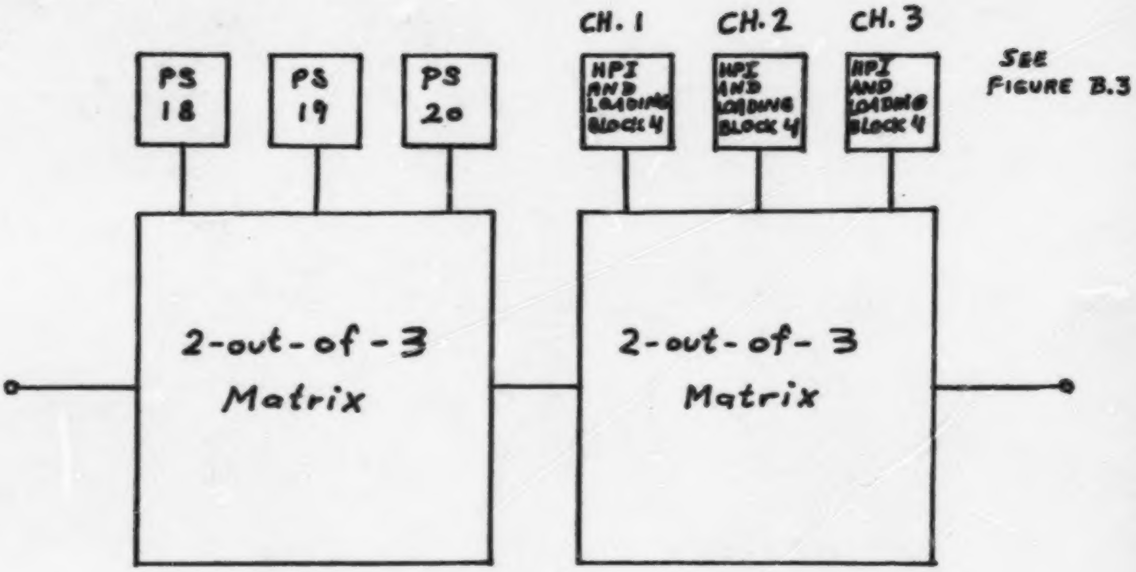

CH. 1
CH. 2
CH. 3
PS 18
PS 19
PS 20
HPI AND LOADING BLOCK 4
HPI AND LOADING BLOCK 4
HPI AND LOADING BLOCK 4
SEE FIGURE B.3
2-out-of-3 Matrix
2-out-of-3 Matrix

Figure B.5 ESAS - Reactor Building Spray Actuation (1 Train)

B.2 SYSTEM SIMPLIFIED FAULT TREE

Fault trees were constructed to model ESAS failure to actuate ESF equipment during LOCAs. The ESAS responds to a B_4 LOCA by actuating the HPI equipment group (including the LPI pumps). All other ESF functions (LPI injection line valves, RBIC, and RBSS) are not actuated. If a larger LOCA (B_1, B_2, or B_3) is the initiating event, it is expected that all ESF equipment will be given actuation signals.

A set of two fault trees was constructed for ESAS failure to actuate HPI, given a B_4 LOCA. One top event is defined as the failure of a single piece of HPI equipment to receive an actuation signal from the ESAS (Event ISS). This top event is necessary to provide an interface to individual equipment appearing in system fault trees. Evaluation of this tree provides a failure-to-actuate probability for use in conjunction with individual equipment failures appearing in the HPI system fault tree. The fault tree structure developed in this tree is valid for both immediate and loading sequence time delayed equipment actuation. The differences in circuitry involved are taken into account by modifying the unavailabilities of the group logic and the output relay to reflect the differences in hardware configuration.

The top event for the second fault tree for ESAS to actuate HPI, given a B_4 LOCA, is defined as failure of both HPI actuation trains to generate actuation signals (Event ISB). Evaluation of this tree provides the probability that equipment in both HPI trains will not be actuated. This event appears as a common mode fault in the HPI system fault trees.

A second set of two fault trees similar to those described above, was constructed for ESAS failure to actuate each ESF, given a B_1, B_2, or B_3 LOCA (Events ILB and ILS). The basic fault tree structure for these trees is defined by the fact that all ESF equipment is actuated by providing continuity to control circuits with two-out-of-three relay matrices. Each type of actuation circuit, however, contains a slightly different equipment configuration which is included in the models. In addition, these models include a common mode human error for actuation of the RBIC and RBSS. This error is the miscalibration of all pressure switches and pressure regulators used to test pressure switches.

The detailed fault trees were simplified by the elimination of failure combinations containing more than two active failures, since these fault combinations are not expected to contribute to the system failure. The resulting simplified fault trees for ESAS failure to actuate HPI, given a B_4 LOCA, are shown in Figures B.6 and B.7; those for ESAS failure to actuate each ESF, given a B_1, B_2, or B_3 LOCA*, are shown in Figures B.8 and B-9. The top event definitions for the simplified fault trees are shown in Table B.3.

---

*The RBSS pumps do not receive an ESAS actuation signal from the B_3 LOCA initiator; however, the spray line injection valves are actuated (opened) by the RB 4 psi trip signal.

BEST DOCUMENT AVAILABLE

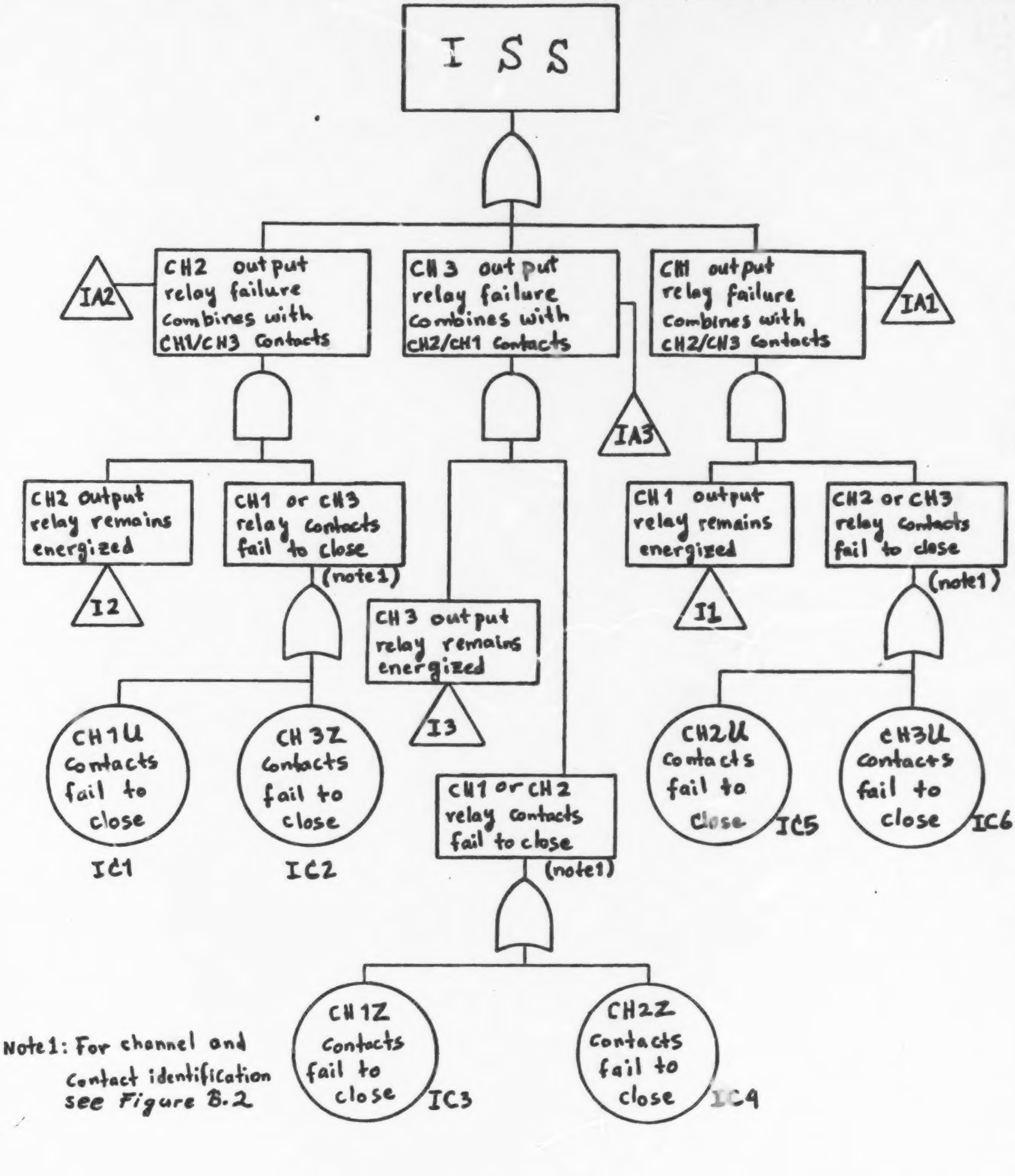
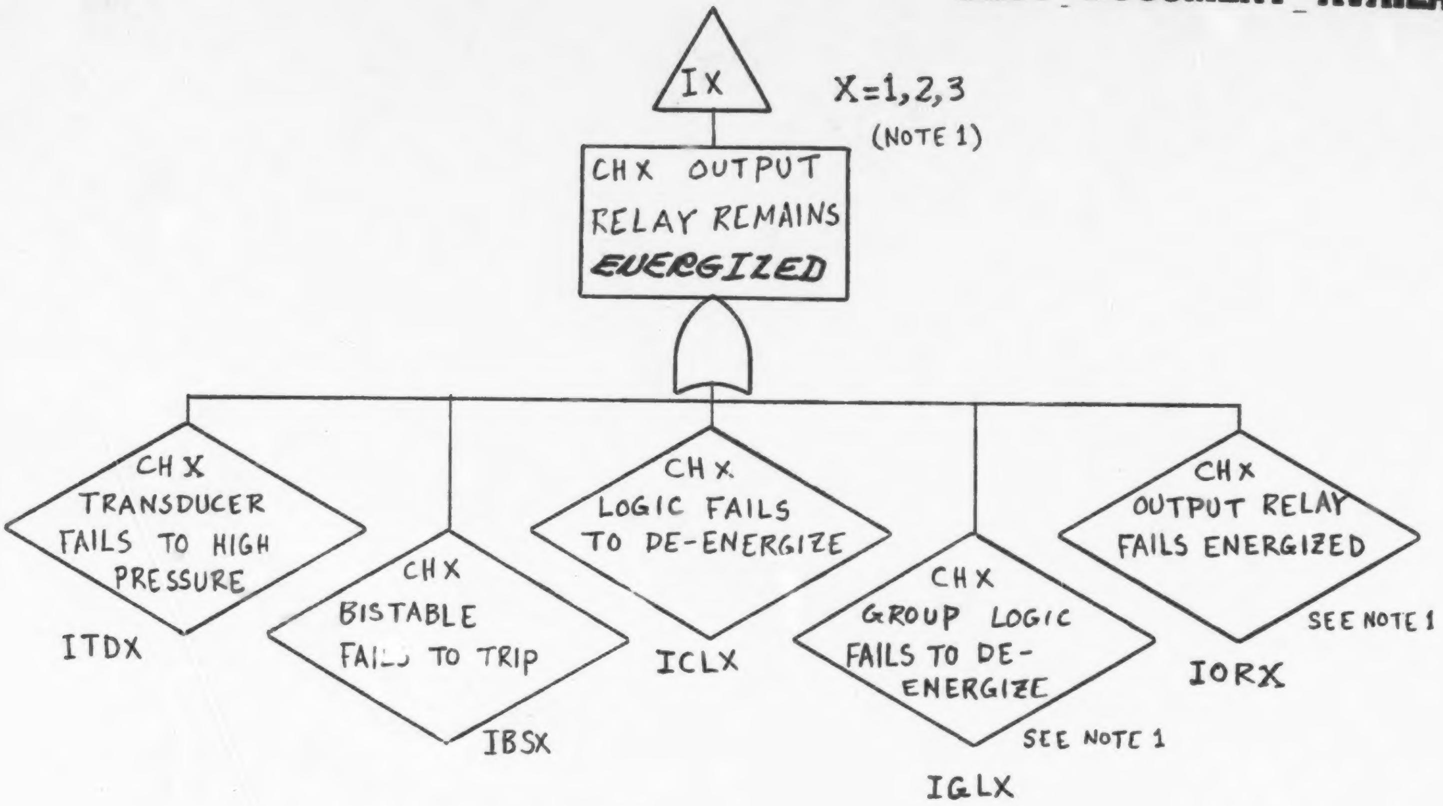

ISS
IA2
CH2 output relay failure combines with CH1/CH3 Contacts
CH3 output relay failure combines with CH2/CH1 Contacts
CH1 output relay failure combines with CH2/CH3 Contacts
IA1
IA3
CH2 output relay remains energized
I2
CH1 or CH3 relay contacts fail to close
(note1)
CH3 output relay remains energized
I3
CH1 output relay remains energized
I1
CH2 or CH3 relay contacts fail to close
(note1)
CH1U Contacts fail to close
IC1
CH3Z Contacts fail to close
IC2
CH1 or CH2 relay contacts fail to close
(note1)
CH2U contacts fail to close
IC5
CH3U contacts fail to close
IC6
CH1Z Contacts fail to close
IC3
CH2Z Contacts fail to close
IC4
Note1: For channel and contact identification see Figure B.2

Figure B.6 (1/2) Simplified Fault Tree - ESAS (Event "ISS", B_4 LOCA)

BEST DOCUMENT AVAILABLE


IX
X=1,2,3
(NOTE 1)
CHX OUTPUT RELAY REMAINS ENERGIZED
CHX TRANSDUCER FAILS TO HIGH PRESSURE
ITDX
CHX BISTABLE FAILS TO TRIP
IBSX
CHX LOGIC FAILS TO DE-ENERGIZE
ICLX
CHX GROUP LOGIC FAILS TO DE-ENERGIZE
SEE NOTE 1
IGLX
CHX OUTPUT RELAY FAILS ENERGIZED
SEE NOTE 1
IORX

NOTE 1 : Unavailability used here depends on equipment configuration; time delay or immediate actuation.

Figure B.6 (2/2) Simplified Fault Tree - ESAS (Event "IX", X = 1, 2, 3; B_4 LOCA)

BEST DOCUMENT AVAILABLE

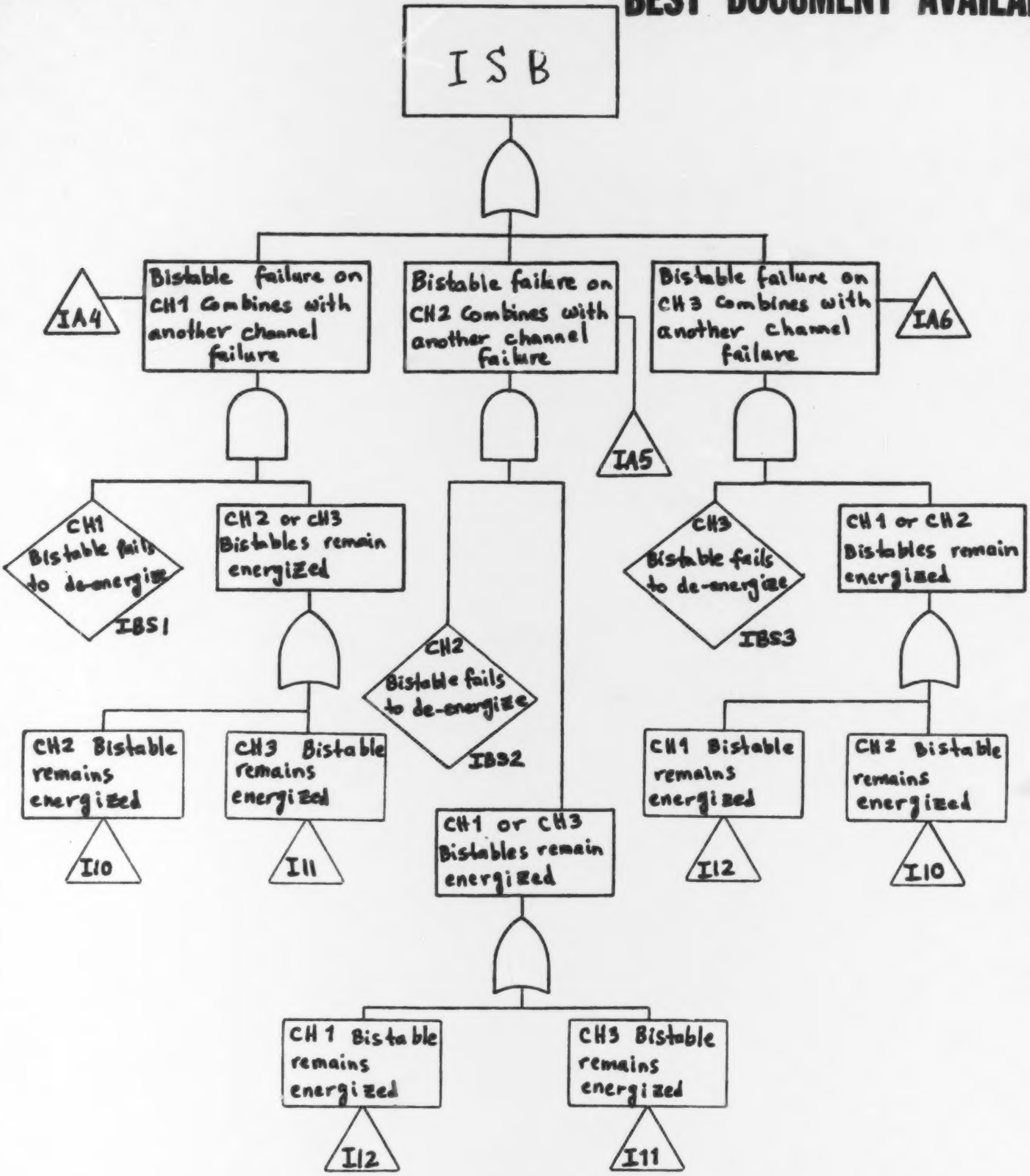

ISB
Bistable failure on CH1 Combines with another channel failure
IA4
Bistable failure on CH2 Combines with another channel failure
IA5
Bistable failure on CH3 Combines with another channel failure
IA6
CH1 Bistable fails to de-energize
IBS1
CH2 or CH3 Bistables remain energized
CH2 Bistable fails to de-energize
IBS2
CH3 Bistable fails to de-energize
IBS3
CH1 or CH2 Bistables remain energized
CH2 Bistable remains energized
I10
CH3 Bistable remains energized
I11
CH1 or CH3 Bistables remain energized
CH1 Bistable remains energized
I12
CH2 Bistable remains energized
I10
CH1 Bistable remains energized
I12
CH3 Bistable remains energized
I11

Figure B.7 (1/2) Simplified Fault Tree - ESAS (Event "ISB"; B_4 LOCA)

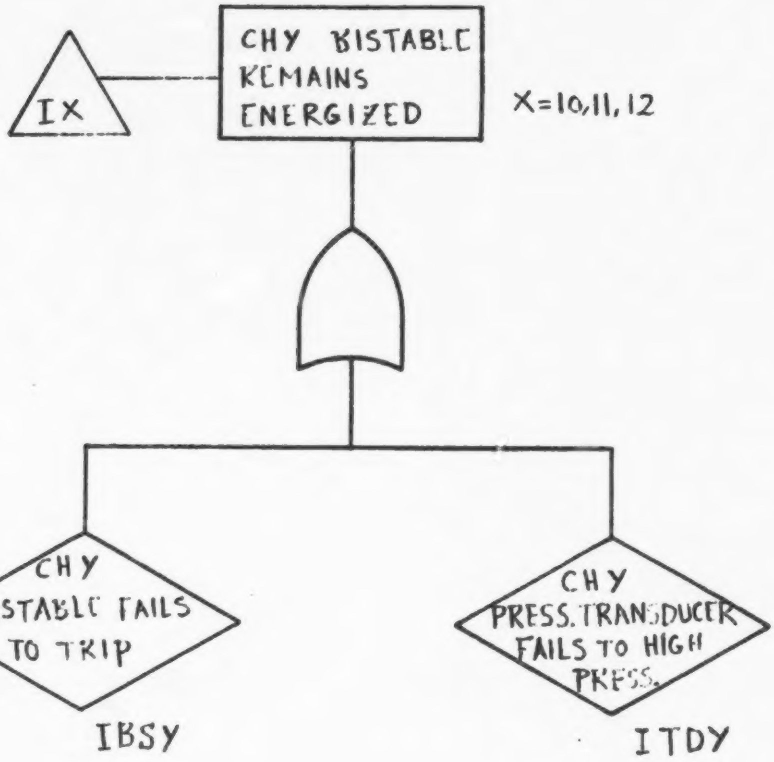
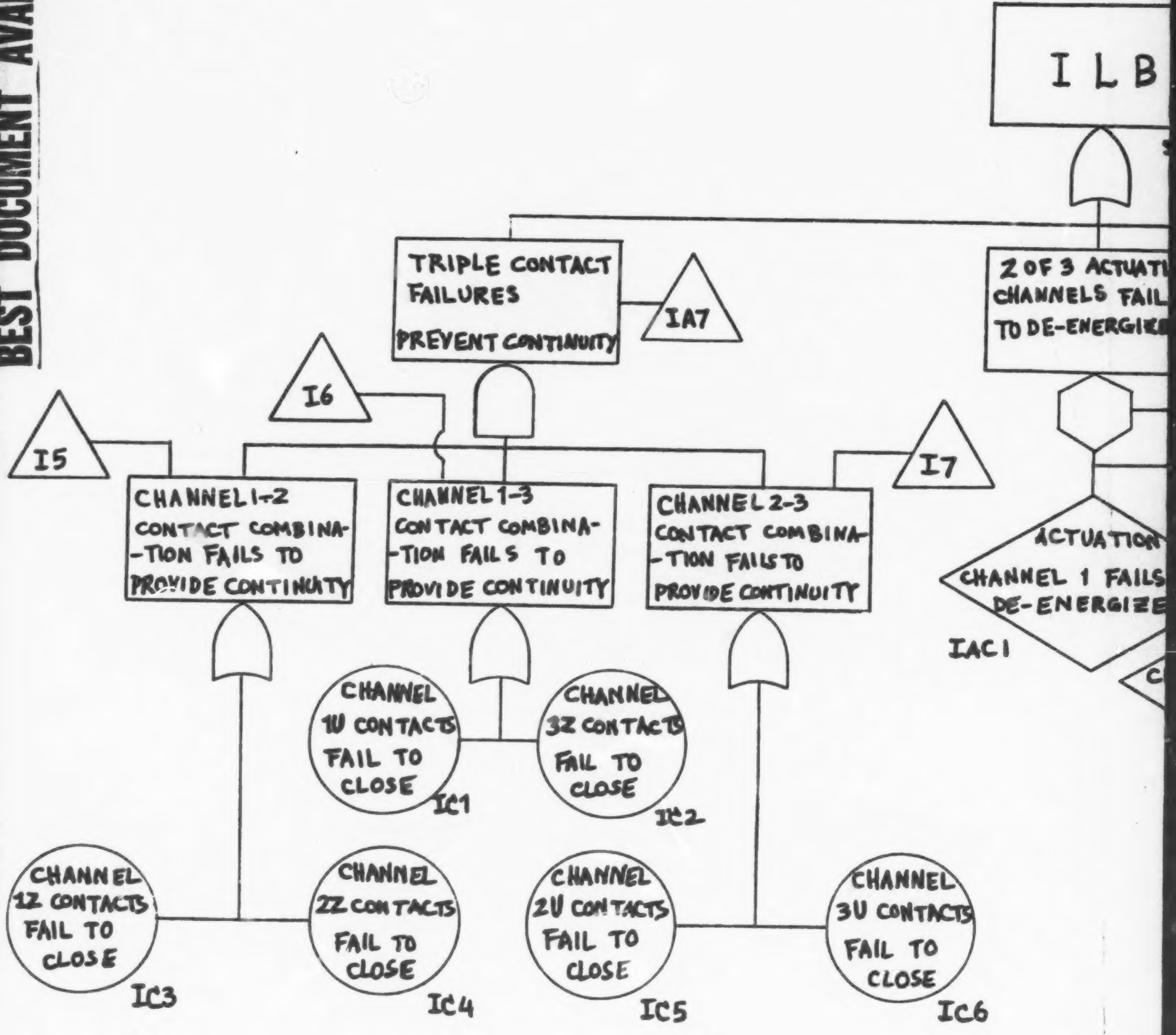

IX
CHY BISTABLE REMAINS ENERGIZED
X=10,11,12
CHY BISTABLE FAILS TO TRIP
IBSY
CHY PRESS. TRANSDUCER FAILS TO HIGH PRESS.
ITDY

Figure B.7 (2/2) Simplified Fault Tree - ESAS (Event "IX", X = 10 and Y = 2, X = 11 and Y = 3, X = 12 and Y = 1; B_4 LOCA)

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE


ILB
TRIPLE CONTACT FAILURES PREVENT CONTINUITY
IA7
2 OF 3 ACTUATI
CHANNELS FAIL
TO DE-ENERGIZE
I6
I5
I7
CHANNEL 1-2 CONTACT COMBINA-TION FAILS TO PROVIDE CONTINUITY
CHANNEL 1-3 CONTACT COMBINA-TION FAILS TO PROVIDE CONTINUITY
CHANNEL 2-3 CONTACT COMBINA-TION FAILS TO PROVIDE CONTINUITY
ACTUATION CHANNEL 1 FAILS DE-ENERGIZE
IAC1
C
CHANNEL 1U CONTACTS FAIL TO CLOSE
IC1
CHANNEL 3Z CONTACTS FAIL TO CLOSE
IC2
CHANNEL 1Z CONTACTS FAIL TO CLOSE
IC3
CHANNEL 2Z CONTACTS FAIL TO CLOSE
IC4
CHANNEL 2U CONTACTS FAIL TO CLOSE
IC5
CHANNEL 3U CONTACTS FAIL TO CLOSE
IC6

BEST DOCUMENT AVAILABLE

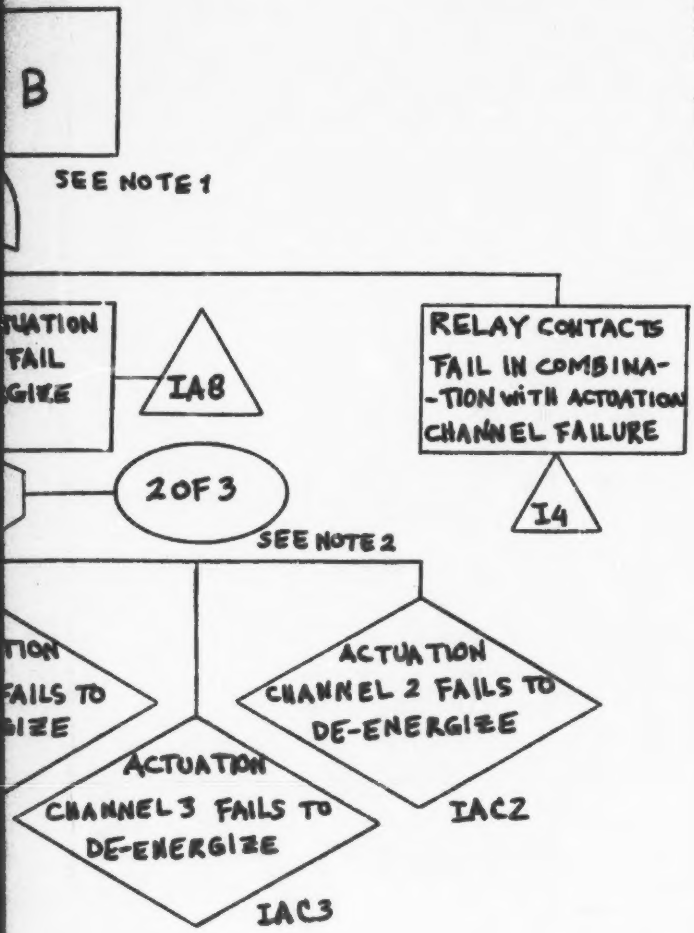

B
SEE NOTE 1
UATION
FAIL
GIZE
IA8
RELAY CONTACTS FAIL IN COMBINA-TION WITH ACTUATION CHANNEL FAILURE
I4
2 OF 3
SEE NOTE 2
TION
FAILS TO
GIZE
ACTUATION CHANNEL 2 FAILS TO DE-ENERGIZE
IAC2
ACTUATION CHANNEL 3 FAILS TO DE-ENERGIZE
IAC3

Figure B.8 (1/2) Simplified Fault Tree - ESAS (Event "ILB"; B_1, B_2, or B_3 LOCA)

BEST DOCUMENT AVAILABLE

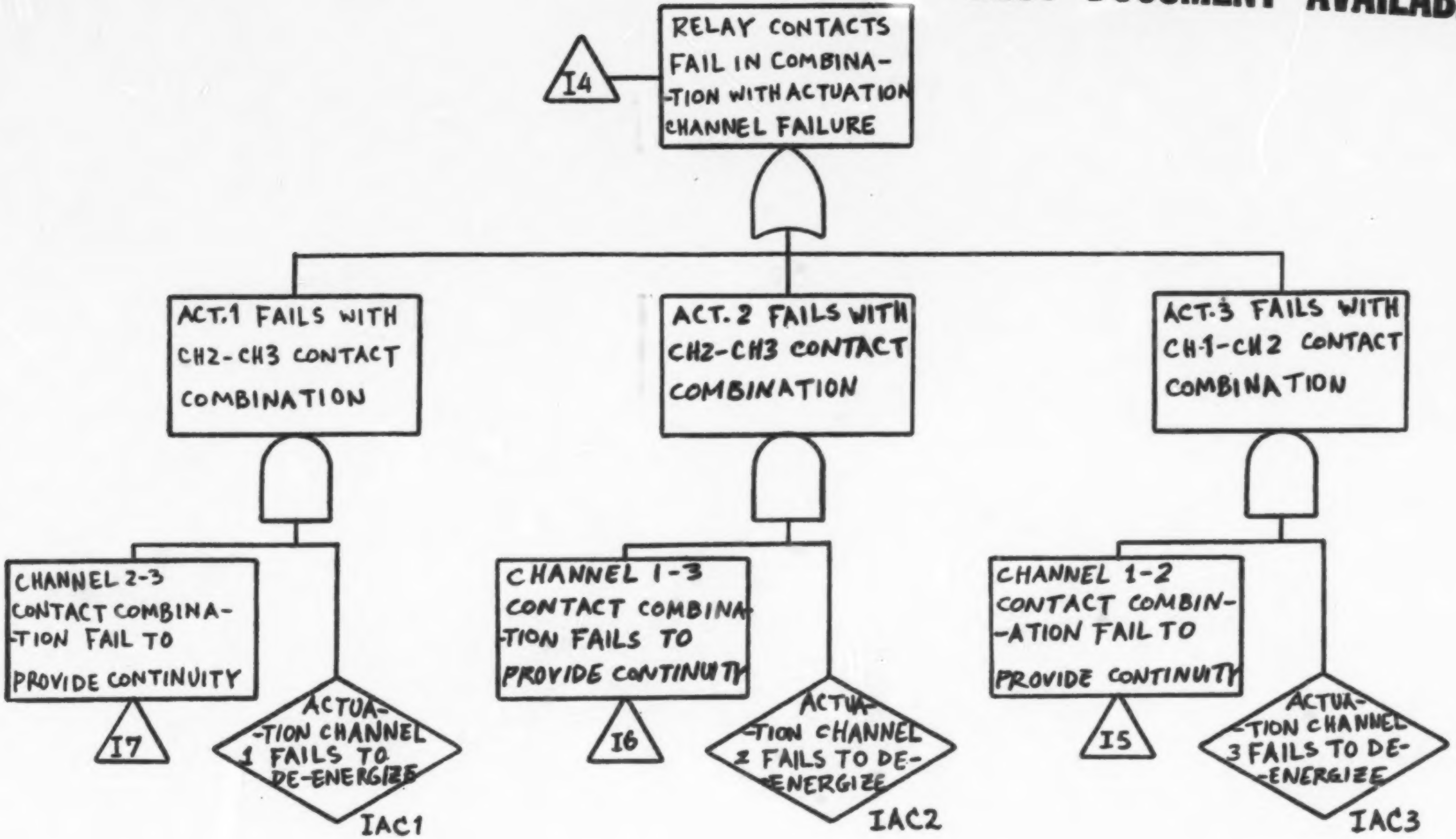

I4
RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE
ACT.1 FAILS WITH CH2-CH3 CONTACT COMBINATION
ACT. 2 FAILS WITH CH2-CH3 CONTACT COMBINATION
ACT.3 FAILS WITH CH1-CH2 CONTACT COMBINATION
CHANNEL 2-3 CONTACT COMBINATION FAIL TO PROVIDE CONTINUITY
I7
ACTUATION CHANNEL 1 FAILS TO DE-ENERGIZE
IAC1
CHANNEL 1-3 CONTACT COMBINATION FAILS TO PROVIDE CONTINUITY
I6
ACTUATION CHANNEL 2 FAILS TO DE-ENERGIZE
IAC2
CHANNEL 1-2 CONTACT COMBINATION FAIL TO PROVIDE CONTINUITY
I5
ACTUATION CHANNEL 3 FAILS TO DE-ENERGIZE
IAC3

Figure B.8 (2/2) Simplified Fault Tree - ESAS (Event "I4"; B_1, B_2 or B_3 LOCA)

Figure B.8 Simplified Fault Tree - ESAS
(Event "ILB")

NOTES:

1 The RBSS pumps do not receive an ESAS actuation signal for the B_3 LOCA initiator; however, the spray line injection valves are actuated (opened).

2 This event is failure of automatic actuation of all equipment in one train.

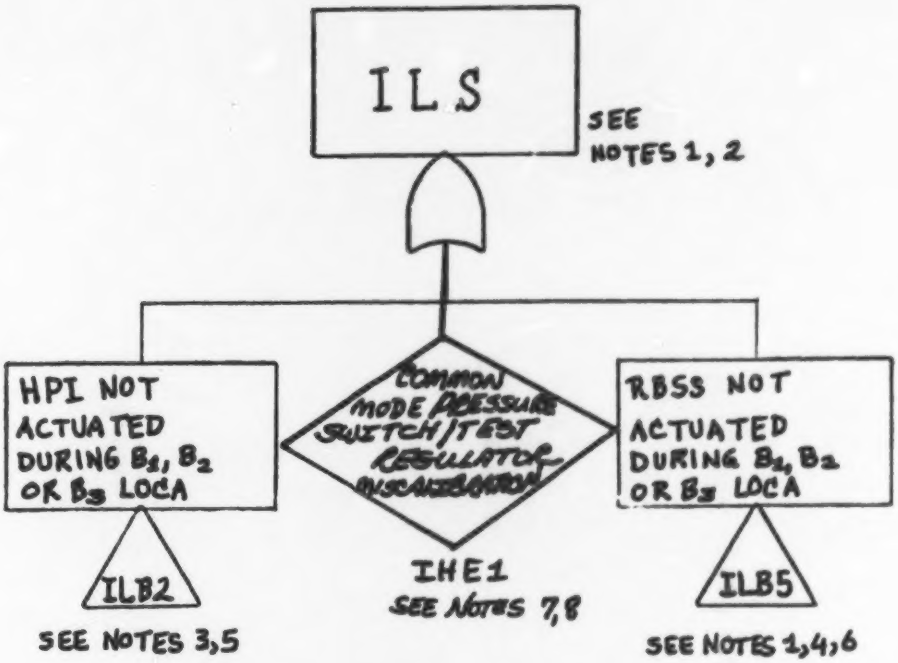

ILS
SEE NOTES 1, 2
HPI NOT ACTUATED DURING B_1, B_2 OR B_3 LOCA
COMMON MODE PRESSURE SWITCH/TEST REGULATOR MISCALIBRATION
RBSS NOT ACTUATED DURING B_1, B_2 OR B_3 LOCA
ILB2
SEE NOTES 3,5
IHE1
SEE NOTES 7,8
ILB5
SEE NOTES 1,4,6

Figure B.9 Simplified Fault Tree - ESAS (Event "ILS"; B_1, B_2 or B_3 LOCA)

Figure B.9 Simplified Fault Tree - ESAS
(Event "ILS")

NOTES

1 The RBSS pumps do not receive an ESAS actuation signal for the B_3 LOCA initiator; however, the spray line injection valves are actuated (opened).

2 This fault tree combines a RBSS and HPI fault tree to model the entire RBSS actuation circuit.

3 ESAS fault tree evaluated for HPI 15 sec time delay (B_1, B_2, or B_3 LOCA).

4 ESAS fault tree evaluated for RBSS switch matrix (B_1, B_2, or B_3 LOCA)

5 See quantification table for event ILB2

6 See quantification table for event ILB5.

7 This event is miscalibration of all pressure switches (both 4 psi and 30 psi) and pressure-switch-test pressure regulators due to a maintenance error during a refueling outage. This event disables the RBSS and RBIC actuation trains because the actuation logic circuit for the RBIC is a required part of the actuation logic circuit for the RBSS. It does not affect the LPI or HPI actuation trains.

8 This event results in failure to actuate all equipment in both trains in RBSS and both trains in RBIC.

B.3 SYSTEM QUANTIFICATION

B.3.1 SYSTEM RELIABILITY CHARACTERISTICS

Table B.3 contains the results of the evaluation of the fault trees for the top events in the ESAS fault trees. The results in most cases are dominated by failures within the ESAS output matrices which provide actuation signals to individual pieces of equipment. Two types of ESAS actuation signal top events shown in the table appear as common mode faults in the fault trees for the systems receiving the actuation signals. The first, for the B_4 LOCA, is "HPI Actuation Signal Not Available to Any Equipment" (Event ISB). The second of these faults, for the B_1, B_2, or B_3 LOCA is "All RBIC, RBSS Systems Do Not Receive Actuation Signal" (Event ILS). This fault can result from equipment miscalibration due to a common-mode human error.

The dominant failure mode for ESAS failure to actuate one piece of HPI equipment, given a B_4 LOCA (Event ISS), is due to combinations of output relay matrix contact failures and failure to trip of a bistable in another channel. The dominant failure mode of both HPI actuation trains, given a B_4 LOCA (Event ISB) is a combination of two bistables failing to trip.

The dominant reason for ESAS failure to actuate LPI, HPI, and RBIC, given a B_1, B_2 or B_3 LOCA, is combinations of three output relay contacts failing to close when their associated relays are de-energized. In addition to the triple contact failure, the time delay HPI actuation system of 1 relay contact failure and failure of the actuation channel is found to be a significant contributor. The common mode pressure switch miscalibration event dominates all failures of the RBIC and RBSS actuation systems. The most likely failure event for automatic actuation of these systems is total loss of actuation signals to both systems (Event ILS).

B.3.2 SYSTEM FAULT TREE QUANTIFICATION

The Engineered Safeguards Actuation System does not depend on any other system (i.e., power failure would cause an ESAS signal). The independence from any other system does not require a Boolean reduction in the event tree sequence analysis. Therefore, no modularized fault tree was constructed. The simplified fault trees presented in Section B.2 are used for the quantification purposes.

Table B.4 shows the ESAS success requirement. Table B.5 contains the top event definitions for the simplified fault trees (Figures B.6 through B.9). Table B.6 shows the Boolean equations that represent the fault trees. Table B.7 shows the quantification of each gate by component and failure mode. Table B.8 summarizes the point estimates of the top events.

Table B.3 Results of ESAS Quantification

INITIATING EVENT	TOP EVENT**	FAULT TREE TOP EVENT	UNAVAILABILITY
B_4 LOCA	ISS1	Non-time delayed HPI actuation signal not available to exactly 1 piece of equipment	2.1×10^{-4}
	ISS2	Time delayed HPI actuation signal not available to exactly 1 piece of equipment	2.2×10^{-4}
	ISB	HPI actuation signal not available to any equipment (Both trains failed)	7.2×10^{-4}
B_1, B_2, or B_3 LOCA	ILB1	Non-time delayed HPI actuation signal not available to exactly 1 piece of equipment	1.0×10^{-7}
	ILB2	Time delayed HPI actuation signal not available to exactly 1 piece of equipment	5.6×10^{-6}
	ILB3	LPI actuation signal not available to exactly 1 piece of equipment	1.0×10^{-7}
	ILB4	RBIC actuation signal not available to exactly 1 piece of equipment	1.3 E-6
	ILB5	Reactor building high pressure signal not available to actuate exactly 1 piece of RBSS equipment*	1.2 E-6
	ILS	All RBIC and RBSS equipment does not receive actuation signal*,*** (ILS=ILB2 + ILB5 + IHE1)	1.1 E-4

---

*The RBSS pumps do not receive an ESAS signal for the B_3 LOCA initiator; however, the spray line injection valves do receive signal.

**The top events for the simplified fault trees, Figures B.6 through B.9, are defined in Table B.5, and quantified in Table B.7.

***The actuation logic circuit for the RBIC is a required part of the actuation logic circuit for the RBSS. Thus, if the RBIC actuation logic circuit fails, the RBSS actuation logic circuit will also fail.

Table B.3 ESAS - System Success Requirements

INITIATOR	TRAINS	NOTES
all	2/3 channels to each equipment	

Table B.5 ESAS - Top Event Definitions

BOOLEAN REPRESENTATION	TOP EVENT	NOTES
ISSa	See below for a equal to 1 or 2	1
ISS1	Non-time delayed HPI actuation signal not available to exactly one piece of equipment (B_4 LOCA)	1
ISS2	Time delayed HPI actuation signal not available to exactly one piece of equipment (B_4 LOCA).	1
ISB	HPI actuation signal not available to any HPI equipment (B_4 LOCA)	
ILBa	See below for a equal to 1, 2, 3, 4 and 5	3
ILB1	Non-time dependent HPI signal not available to exactly one piece of equipment (B_1, B_2, B_3 LOCAs)	3
ILB2	Time delayed HPI actuation signal not available to exactly one piece of equipment (B_1, B_2, B_3 LOCAs)	3
ILB3	LPI actuation signal not available to exactly one piece of equipment (B_1, B_2, B_3 LOCAs)	3
ILB4	RBIC actuation signal not available to exactly one piece of equipment (B_1, B_2, B_3 LOCA)	3
ILB5	Reactor building high pressure signal not available to actuate exactly one piece of RBSS equipment (B_1, B_2, B_3 LOCAs)	2,3
ILS	All RBIC and RBSS equipment does not receive actuation signal during B_1, B_2, or B_3 LOCAs.	2

Table B.5 ESAS - Top Event Definitions

NOTES

1 The numerical evaluation is different for ISS1 and ISS2; however, the same tree with top event ISS is used.

2 The RBSS pumps do not receive an ESAS actuation signal for the B_3 LOCA initiator; however, the spray line injection valves are actuated (opened).

3 The numerical evaluation is different for ILB1, 2, 3, 4, and 5; however, the same tree with top event ILB is used.

Table B.6 ESAS

BOOLEAN EQUATIONS BASED ON SIMPLIFIED FAULT TREES

TOP EVENTS — **NOTES**

B_4 - LOCA

ISS = ISS1 = ISS2 = IA1 + IA2 + IA3
ISB = IA4 + IA5 + IA6

B_1, B_2, B_3 - LOCAs

ILB = ILBX=I5·I6·I7 + I4+(IAC1·IAC2 +
+ IAC1·IAC3 + IAC2·IAC3) (1)
for X = 1,2,3,4,5

ILS = ILB2 + ILB5 + IHE1 (4)

INTERMEDIATE EVENTS

B_4 - LOCA

IA1 = I1·(IC5 + IC6)
IA2 = I2·(IC1 + IC2)
IA3 = I3·(IC3 + IC4)

IX = ITDX + IBSX + ICLX + IGLX + IORX (2)
for X = 1,2,3
IA4 = IBS1·(I10 + I11)
IA5 = IBS2·(I11 + I12)
IA6 = IBS3·(I10 + I12)

IX = IBSY + ITDY (3)
for X = 10 and Y = 2, X = 11 and Y = 3, X = 12 and Y = 1

B_1, B_2, B_3 - LOCA

I4 = IAC1·I7 + IAC2·I6 + IAC3·I5

I5 = IC3 + IC4
I6 = IC1 + IC2
I7 = IC5 + IC6

Table B.6 ESAS

BOOLEAN EQUATIONS BASED ON SIMPLIFIED FAULT TREE

NOTES

1 The expression in parenthesis reflects the possible "2-out-of-3" failure combinations.

2 For further definition of the parameter "X" see also quantification tables.

3 For further definition of the parameters "X" and "Y" see also quantification tables.

4 Event IHE1 contributes only to ILB4 and ILB5.

Table B.7 (1/9) Event "ISS1" Quantification (B_4 LOCA, Non Time Delayed)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ISS1		NON-TIME DEPENDENT HPI SIGNAL NOT AVAILABLE TO EXACTLY ONE PIECE OF EQUIPMENT DURING B_4 LOCA			2.1 E-4			
IA1		CHANNEL 1 OUTPUT RELAY FAILURE COMBINES WITH CHANNEL 2 AND 3 CONTACT FAILURES			7.0 E-5			
IA2		CHANNEL 2 OUTPUT RELAY FAILURE COMBINES WITH CHANNEL 1 AND 3 CONTACT FAILURES			7.0 E-5			
IA3		CHANNEL 3 OUTPUT RELAY FAILURE COMBINES WITH CHANNEL 1 OR CHANNEL 2 CONTACT FAILURES			7.0 E-5			
					Σ= 2.1 E-4			
IAX		CHANNEL X OUTPUT RELAY FAILURE COMBINES WITH CHANNEL Y OR CHANNEL Z CONTACT FAILURES			7.0 E-5			1
ICY	CH. UA	CHANNEL U/CONTACT A FAILS TO CLOSE	1.0 E-7	1.9 E+4	1.9 E-3	10^+, 10^-		1, 2, 3
ICZ	CH. VB	CHANNEL V/CONTACT B FAILS TO CLOSE	1.0 E-7	1.9 E+4	1.9 E-3	10^+, 10^-		1, 2, 3
					Σ= 3.9 E-3			
IX	CH. X OUTPUT RELAY	REMAINS ENERGIZED			1.8 E-2			
ITDX	CH. X TRANSDUCER	FAILS TO HIGH PRESSURE (SHIFT IN CALIBRATION)	3.0 E-5	4	1.2 E-4	10^+, 10^-		
IBSX	CH. X BISTABLE	FAILS TO TRIP (SET POINT DRAFT)	3.0 E-5	360	1.1 E-2	10^+, 10^-		
ICLX	CH. X LOGIC	FAILS TO DE-ENERGIZE (2 SWITCHES)	(2)(1.0 E-5)	360	7.2 E-3	3^+, 3^-		
IGLX	CH. X GROUP LOGIC	FAILS TO DE-ENERGIZE	1.0 E-8	360	3.6 E-6	10^+, 10^-		
IORX	CH. X OUTPUT RELAY	FAILS ENERGIZED	1.0 E-8	360	3.6 E-6	10^+, 10^-		
					Σ=1.8 E-2 π=7.0 E-5			

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table B.7 (2/9) Event "ISS2" Quantification (B_4 LOCA, Non Time Delayed)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ISS2		TIME DELAYED HPI SIGNAL NOT AVAILABLE TO ONE PIECE OF EQUIPMENT DURING B_4 LOCA			2.2 E-4			
IA1		CHANNEL 1 OUTPUT RELAY FAILURE COMBINES WITH CHANNEL 2 AND 3 CONTACT FAILURES			7.4 E-5			
IA2		CHANNEL 2 OUTPUT RELAY FAILURE COMBINES WITH CHANNEL 1 AND 3 CONTACT FAILURES			7.4 E-5			
IA3		CHANNEL 3 OUTPUT RELAY FAILURE COMBINES WITH CHANNEL 1 AND 2 CONTACT FAILURES			7.4 E-5			
					Σ=2.2 E-4			
IAX		CHANNEL X OUTPUT RELAY FAILURE COMBINES WITH CHANNEL Y OR CHANNEL 2			7.4 E-5			1
ICY	CH. UA	CHANNEL U/CONTACT A FAILS TO CLOSE	1.0 E-7	1.9 E+4	1.9 E-3	10^+, 10^-		1, 2, 3
ICZ	CH. VB	CHANNEL V/CONTACT B FAILS TO CLOSE	1.0 E-7	1.9 E+4	1.9 E-3	10^+, 10^-		1, 2, 3
					Σ=3.9 E-3			
IX	CH. X OUTPUT RELAY	REMAINS ENERGIZED			1.9 E-2			
ITDX	CH. X TRANSDUCER	FAILS TO HIGH PRESSURE (SHIFT IN CALIBRATION	3.0 E-5	4	1.2 E-4	10^+, 10^-		
IBSX	CH. X BISTABLE	FAILS TO TRIP (SET POINT DRIFT)	3.0 E-5	360	1.1 E-2	10^+, 10^-		
ICLX	CH. X LOGIC	FAILS TO DE-ENERGIZE (2 SWITCHES)	(2)(1.0 E-5)	360	7.2 E-3	3^+, 3^-		
IGLX	CH. X GROUP LOGIC	FAILS TO DE-ENERGIZE			1.1 E-4			
	1 RELAY COIL	ENERGIZED	1.0 E-8	360	3.6 E-6	10^+, 10^-		
	2 SETS RELAY CONTACTS	FAILURE OF N.O. CONTACTS TO OPEN	1.0 E-8	360	3.6 E-6	10^+, 10^-		
	1 RELAY	FAILS TO ENERGIZE	D		1.0 E-4	3^+, 3^-		
					Σ=1.1 E-4			
IORX	OUTPUT RELAY	FAILS ENERGIZED			3.7 E-4			
	1 RELAY COIL	ENERGIZED	1.0 E-8	360	3.6 E-6	10^+, 10^-		
	1 SET RELAY CONTACTS	FAILURE OF N.O. CONTACTS TO OPEN	1.0 E-8	360	3.6 E-6	10^+, 10^-		
	1 TIME DELAY	FAILS TO DE-ENERGIZE	1.0 E-6	360	3.6 E-4			
					Σ=3.7 E-4			

Table B.7 (3/9) Event "ISB" Quantification (B_4 LOCA)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ISB		HPI ACTUATION SIGNAL NOT AVAILABLE TO ANY EQUIPMENT DURING B_4 LOCA			7.2 E-4			
IA4		BISTABLE FAILURE ON CHANNEL 1 COMBINES WITH ANOTHER CHANNEL FAILURE			2.4 E-4			
IA5		BISTABLE FAILURE ON CHANNEL 2 COMBINES WITH ANOTHER CHANNEL FAILURE			2.4 E-4			
IA6		BISTABLE FAILURE ON CHANNEL 3 COMBINES WITH ANOTHER CHANNEL FAILURE			2.4 E-4			
					Σ=7.2 E-4			
IAX		BISTABLE FAILURE ON CHANNEL X COMBINES WITH ANOTHER CHANNEL FAILURE			2.4 E-4			4
IBSY		SEE EVENT "ISS" QUANTIFICATION			1.1 E-2	10^+, 10^-		4
ITDY		SEE EVENT "ISS" QUANTIFICATION			1.2 E-4	10^+, 10^-		4
IBSZ		SEE EVENT "ISS" QUANTIFICATION			1.1 E-2	10^+, 10^-		4
ITDZ		SEE EVENT "ISS" QUANTIFICATION			1.2 E-4	10^+, 10^-		4
					Σ=2.2 E-2			
IBSU		SEE EVENT "ISS" QUANTIFICATION			1.1 E-2	10^+, 10^-		
					π=2.4 E-4			

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table B.7 (4/9) Event ILB1" Quantification (B_1, B_2 LOCA, Non-Time Dependent)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ILB1		NON-TIME DEPENDENT HPI SIGNAL NOT AVAILABLE TO EXACTLY ONE PIECE OF EQUIPMENT DURING B_1, B_2 OR B_3 LOCA			1.0 E-7			
IA7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			5.9 E-8			
IA8		2-OUT-OF-3 ACTUATION CHANNELS FAIL TO DE-ENERGIZE						
I4		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			4.2 E-8			
					Σ= 1.0 E-7			
IA7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			5.9 E-8			7
IX		CHANNEL 1 OR 2 CONTACT COMBINATIONS FAIL TO PROVIDE CONTINUITY			3.9 E-3			6
ICY	CH. UA	FAILS TO CLOSE	1.0 E-7	1.9 E+4	1.9 E-3	10^+, 10^-		2, 3, 6
ICZ	CH. VA	FAILS TO CLOSE	1.0 E-7	1.9 E+4	1.9 E-3	10^+, 10^-		2, 3, 6
					Σ= 3.9 E-3			
I4		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			4.2 E-8			8
IAC1	1 RELAY COIL	ENERGIZED (ACTUATION CHANNEL 1)	1.0 E-8	360	3.6 E-6			
I7		SEE ABOVE EVENT "IX"			3.9 E-3			
					π=1.4 E-8			

Table B.7 (5/9) Event "ILB2" Quantification (B_1, B_2 LOCA, Time Delayed)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ILB2		TIME DELAYED HPI SIGNAL NOT AVAILABLE TO EXACTLY ONE PIECE OF EQUIPMENT DURING B_1, B_2 OR B_3 LOCA			5.6 E-6			
IA7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			5.9 E-8			
IA8		2-OUT-OF-3 ACTUATION CHANNELS FAIL TO DE-ENERGIZE			ε			
I4		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			5.5 E-6			
					Σ=5.6 E-6			
IA7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			5.9 E-8			7
IX		CHANNEL 1 OR 2 CONTACT COMBINATIONS FAIL TO PROVIDE CONTINUITY			3.9 E-3			6
ICY	CH. UA	FAILS TO CLOSE	1.0 E-7	1.9 E+4	1.9 E-3	10^+, 10^-		2, 3, 6
ICZ	CH. VB	FAILS TO CLOSE	1.0 E-7	1.9 E+4	1.9 E-3	10^+, 10^-		2, 3, 6
					Σ=3.9 E-3			
I4		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			5.5 E-6			8
IAC1		ENERGIZED (ACTUATION CHANNEL 1)			4.7 E-4	10^+, 10^-		
	2 RELAY COILS	ENERGIZED	1.0 E-8	360	3.6 E-6	10^+, 10^-		
	2 SETS RELAY CONTACTS	FAILURE OF N.O. CONTACT TO OPEN	1.0 E-8	360	3.6 E-6	10^+, 10^-		
	1 TIME DELAY	FAILS TO OPERATE	1.0 E-6	360	3.6 E-4	10^+, 10^-		
	1 RELAY	FAILS TO ENERGIZE	D		1.0 E-4	3^+, 3^-		
					Σ=4.7 E-4			
I7		SEE ABOVE EVENT "IX"			3.9 E-3			
					π=1.8 E-6			

BEST DOCUMENT AVAILABLE

Table B.7 (6/9) Event "ILB3" Quantification (B_1, B_2 LOCA)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ILB3		LPI SIGNAL NOT AVAILABLE TO EXACTLY ONE PIECE OF EQUIPMENT DURING B_1, B_2 OR B_3 LOCA			1.0 E-7			
IA7		TRIPLE CONTACT FAILURES PERMIT CONTINUITY			5.9 E-8			
IA8		2-OUT-OF-3 ACTUATION CHANNELS FAIL TO DE-ENERGIZE			ε			
I4		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			4.2 E-8			
					Σ=1.0 E-7			
IA7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			5.9 E-8			7
IX		CHANNEL 1 OR 2 CONTACT COMBINATIONS FAILS TO PROVIDE CONTINUITY			3.9 E-3			6
ICY	CH. UA	FAILS TO CLOSE	1.0 E-7	1.8 E+5	1.9 E-3	10^+, 10^-		2, 3, 6
ICZ	CH. VB	FAILS TO CLOSE	1.0 E-7	1.8 E+5	1.9 E-3	10^+, 10^-		2, 3, 6
					Σ=3.9 E-3			
I4		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			4.2 E-8			8
IAC1	1 RELAY COIL	ENERGIZED (ACTUATION CHANNEL 1)	1.0 E-8	360	3.6 E-6	10^+, 10^-		
I7		SEE ABOVE EVENT "IX"			3.9 E-3			
					π=1.4 E-8			

Table B.7 (7/9) Event ILB4" Quantification (B_1, B_2 LOCA)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ILB4		RBIC SIGNAL NOT AVAILABLE TO EXACTLY ONE PIECE OF EQUIPMENT DURING B_1, B_2 OR B_3 LOCA			1.3 E-6			
IA7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			5.9 E-8			
IA8		2-OUT-OF-3 ACTUATION CHANNELS FAIL TO DE-ENERGIZE			ε			
I4		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			1.3 E-6			
					Σ=1.3 E-6			
IA7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			5.9 E-8			7
IX		CHANNEL 1 OR 2 CONTACT COMBINATIONS FAILS TO PROVIDE CONTINUITY			3.9 E-3			6
ICY	CH. UA	FAILS TO CLOSE	1.0 E-7	1.9 E+4	1.9 E-3	10^+, 10^-		2, 3, 6
ICZ	CH. VB	FAILS TO CLOSE	1.0 E-7	1.9 E+4	1.9 E-3	10^+, 10^-		2, 3, 6
					Σ= 3.9 E-3			
I4		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			1.3 E-6			8
IAC1		ENERGIZED (ACTUATION CHANNEL 1)			1.1 E-4			
	3 RELAY COILS	ENERGIZED	1.0 E-8	360	3.6 E-6			
	2 SETS RELAY CONTACTS	FAILURE OF N.O. CONTACT TO OPEN	1.0 E-8	360	3.6 E-6			
	1 PRESSURE SWITCH	FAILURE TO ACTUATE	D		1.0 E-4			
					Σ=1.1 E-4			
I7		SEE ABOVE EVENT "IX"			3.9 E-3			
					π=4.3 E-7			

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table B.7 (8/9) Event "ILB5" Quantification (B_1, B_2 LOCA)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR-1)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ILB5		REACTOR BUILDING HIGH PRESSURE SIGNAL NOT AVAILABLE TOEXACTLY ONE PIECE OF RBSS EQUIPMENT DURING B_1, B_2 OR B_3 LOCA			1.2 E-6			
IA7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			5.9 E-8			
IA8		2-OUT-OF-3 ACTUATION CHANNELS FAIL TO DE-ENERGIZE			ε			
I4		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			1.2 E-6			
					Σ=1.2 E-6			
IA7		TRIPLE CONTACT FAILURES PREVENT CONTINUITY			5.9 E-8			7
IX		CHANNEL 1 OR 2 CONTACT COMBINATIONS FAILS TO PROVIDE CONTINUITY			3.9 E-3			6
ICY	CH. UA	FAILS TO CLOSE	1.0 E-7	1.9 E-4	1.9 E-3	10^+, 10^-		2, 3, 6
ICZ	CH. VB	FAILS TO CLOSE	1.0 E-7	1.9 E-4	1.9 E-3	10^+, 10^-		2, 3, 6
					Σ= 3.9 E-3			
I4		RELAY CONTACTS FAIL IN COMBINATION WITH ACTUATION CHANNEL FAILURE			1.2 E-6			8
IAC1	PRESSURE SWITCH	FAILS TO ACTUATE	D		1.0 E-4	10^+, 10^-		
I7		SEE ABOVE EVENT "IX"			3.9 E-3			
					Σ=3.9 E 7			

Table B.7 (9/9) Event "ILS" Quantification (B_1, B_2 LOCA)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ILS		ALL RBIC AND RBSS EQUIPMENT DOES NOT RECEIVE ACTUATION SIGNAL DURING B_1, B_2 OR B_3 LOCA			1.1 E-4			
ILB5		RB HIGH PRESSURE SIGNAL NOT AVAILABLE TO RBSS EQUIPMENT			1.2 E-6			
ILB2		TIME DELAYED HPI SIGNAL NOT AVAILABLE			5.6 E-6			
THE1	ALL 4 PSI AND 30 PSI PRESSURE SWITCHES	COMMON MODE MISCALIBRATION OF ALL PRESSURE SWITCHES			1.0 E-4 Σ=1.1 E-4			

BEST DOCUMENT AVAILABLE

Table B.7 ESAS

QUANTIFICATION TABLES

NOTES

1 X = 1,2,3; if X = 1 then Y = 5, Z = 6, UA = 2A, VB = 3A
X = 2 then Y = 1, Z = 2, UA = 1A, VB = 3B
X = 3 then Y = 3, Z = 4, UA = 1B, VB = 2B

2 The failure rate of 1.0 E-7/hour is the lower bound of the failure rate given in Appendix III of WASH-1400. The fault duration time of 27 months (1/2 of once every three refuelings-54 months) is based on a review of plant procedure SP-417. According to this procedure, these relays are tested every refueling (18 months) by closing the contacts in one out of three paths through the actuation matrices. Thus, every three refuelings, all contacts in the actuation matrices are tested.

3 For channel and contact identification see Figure B.2

4 X = 4,5,6; if X = 4 then Y = 2, Z = 3, U = 1
X = 5 then Y = 1, Z = 3, U = 2
X = 6 then Y = 1, Z = 2, U = 3

5 Failure of one channel is (1.E-8/hr) (360 hrs) =
= 3.6E-6; therefore 2-out-of-3 is approximately ε.

6 X = 5,6,7; if X = 5 then Y = 3, Z = 4, UA = 1B, VB = 2B
X = 6 then Y = 1, Z = 2, UA = 1A, VB = 3B
X = 7 then Y = 5, Z = 6, UA = 2A, VB = 3A

7 IA7 = I5·I6·I7

8 I4 = IAC1·I7 + IAC2 I6 + IAC3·15; where
IAC1 = IAC2 = IAC3 and I5 = I6 = I7
therefore p(I4) was assessed equal to
(3)p(IAC1).p(I7)

Table B.8 ESAS - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
ISS1	2.1 x E-4
ISS2	2.2 x E-4
ISB	7.2 x E-4
ILB1	1.0 x E-7
ILB2	5.6 x E-6
ILB3	1.0 x E-7
ILB4	1.3 E-6
ILB5	1.2 E-6
ILS	1.1 E-4

APPENDIX C

DC POWER SYSTEM

APPENDIX C DC POWER SYSTEM

C.1 SYSTEM DESCRIPTION AND OPERATION

The DC power system (DCPS), which consists of two isolated buses, provides a continuous source of 250V and 125V DC power for DC pump motors, control, and instrumentation.

The 250V supply provides power to the DC pump motors and certain motor operated valves. The 125V supply provides power for control and instrumentation functions.

C.1.1 SYSTEM DESCRIPTION

Figure C.1 shows a simplified schematic diagram of the CR-3 DC power system.

The DCPS consists of two separate and independent 250/125V DC supplies, each of which includes a battery and associated battery chargers and DC distribution panels.

Each 250/125V DC supply includes two 125V batteries wired to produce one 250V source and two 125V sources. A battery charger is provided for each 125V battery section. A spare charger is also provided as backup to the primary chargers and its output may be fed to either of the 125V battery sections.

DC power from each 250/125V supply is distributed to the various user equipment via distribution panels including a main panel and seven individual panels. The outputs of the batteries and chargers are fed to the main panel where the DC power is, in turn, fed to the individual panels for distribution to the user equipments. The vital inverters are fed directly from the main panel.

Each battery charger is sized to continuously deliver 200 amperes to its associated battery section at 125VDC. Input power to the chargers consists of 480VAC, 1ø from motor control centers. MCC3A-1 feeds chargers A, C and E (spare) which serve 250/125VDC supply 3A and MCC3B-2 feeds chargers B, D and F (spare) which serve 250/125VDC supply 3B. Switches are provided at the input and output of each charger to permit off-line test and maintenance. In addition, fuses at the input and output of each charger provide overload protection.

Each 125V battery section consists of 58 cells rated at 2.2 volts/cell minimum. The capacity of each 250/125V battery supply provides the capability to deliver the loads listed in Tables C.1 and C.2 continuously for two hours and perform three complete cycles of safeguards breaker closures with subsequent tripping (1020 ampere-hours).

The distribution panels consist of switches, fuses and associated wiring for DC power distribution. The switches provide the capability for on-line checkout of user equipment as well as general maintenance and checkout of various elements of the DC system by permitting disconnection from power. The fuses provide overload protection for the DC supply and user equipment.

C.1.2 SYSTEM OPERATION

During normal plant operation the battery chargers supply the normal DC loads while maintaining float charge on the batteries. In the event of loss of AC input to the chargers the batteries will automatically supply the required DC loads.

A high and low voltage alarm is provided in the control room via high/low voltage relay contact closures. The high alarm is set at 137VDC to protect against battery overcharging during normal plant operation. The low voltage alarm is set at 210VDC for DC motor bus voltage and 121VDC for instrumentation and control bus voltage.

Battery discharge is monitored by contact making ammeters located in the main DC panels. This provides a remote alarm when the battery is supplying power to the user equipments.

In the event that a primary charger becomes unavailable due to malfunction, test or maintenance the spare charger is manually switched on-line. This will maintain the float charge on the battery section and supply the DC loads associated with the unavailable charger.

BATTERY TEST AND MAINTENANCE

The individual 125 volt battery sections are given the following tests and inspections:

(a) The voltage, specific gravity and electrolyte level of each cell are measured once each quarter.

(b) During refueling each battery is inspected for physical damage and integrity of intercell connections.

(c) Battery discharge is monitored continually via the contact making ammeters.

(d) Maintenance is performed on the batteries as required to correct for defects.

BATTERY CHARGER TEST AND MAINTENANCE

The individual battery chargers are given the following tests and inspections:

(a) During refueling each charger is demonstrated to be operable via an eight hour load test.

(b) Maintenance is performed on the chargers as required to correct for defects. During maintenance the defective charger is taken off-line and replaced by the spare charger.

(c) Charger performance is continually monitored via high/low voltage alarms in the control room.

Table C.1 Battery 3A Loads (DC unavailable) from CR-3 FSAR

Load Description	Volts	Hp/KVA	Cycle Time(min.)	No. of Breakers
Feedwater Pump 3B Turbine Emergency Oil Pump	250	5 Hp	0-10	
Feedwater Booster Pump 3B Emergency Oil Pump	250	5 Hp	0-10	
Reactor Coolant Pump DC Oil Lift Pump	250	3 Hp	0-60	
Reactor Coolant Pump DC Oil Lift Pump	250	3 Hp	0-60	
Turbine Generator Air Side Seal Oil Pump	250	25 Hp	60-120	
Emergency Diesel Generator Fuel Transfer Pump	250	1 Hp	1-20	
Makeup Pump 3B Lube Oil Pump	250	1 Hp	0-20	
Makeup Pump 3C Lube Oil Pump	250	1 Hp	0-20	
Motor Driven Pump to Hotwell Isolation Valve	250	.09 Hp	10-11	
Auxiliary Feedwater Pump Turbine Steam Supply Isolation Valve	250	1.81 Hp	10-11	
Alterrex Excitation Cabinet	125	6.25 Hp	0-120	
Feedwater Pump 3B Turbine Motor Speed Changer	125	1/6 Hp	0-10	
6900 Volt Switchgear 3B Control	125	*		3
4160 Volt Switchgear 3B Control	125	*		10
4160 Volt Engineered Safeguards Switchgear 3B Control	125	*		10
480 Volt Reactor Auxiliary Bus 3B Control	125	*		2
480 Volt Turbine Auxiliary Bus 3B Control	125	*		7
480 Volt Intake Auxiliary Bus 3B Control	125	*		4
480 Volt Engineered Safeguards Bus 3B Control	125	*		3
Inverter 3B	125	15 KVA	0-120	
Inverter 3D	125	15 KVA	0-120	
Inverter 3E	125	15 KVA	0-120	
Control Room Panels	125	1.25 KVA	0-120	
Hydrogen Panel	125	.625 KVA	0-120	
Engineered Safeguards Channel 3B Cabinets	125	.625 KVA	0-120	
Relay Racks	125	12.5 KVA	0-120	
Engineered Safeguards Actuation 3B Cabinets	125	.625 KVA	0-120	
Emergency Lighting	125	1.25 KVA	0-120	
Substation Loads	125	7.5 KVA	0-120	
Miscellaneous Cabinets	125	1.25 KVA	0-120	

*Power Required to trip breakers as listed (10 amps/breaker for one minute).

Table C.2 Battery 3B Loads (AC unavailable) from CR-3 FSAR

Load Description	Volts	Hp/KVA	Cycle Time(min.)	No. of Breakers
Turbine Emergency Bearing Oil Pump	250	60 Hp	10-60	
Feedwater Pump 3A Turbine Emergency Oil Pump	250	5 Hp	0-10	
Feedwater Booster Pump 3A Emergency Oil Pump	250	5 Hp	0-10	
Reactor Coolant Pump DC Oil Lift Pump	250	3 Hp	0-60	
Reactor Coolant Pump DC Oil Lift Pump	250	3 Hp	0-60	
Emergency Diesel Generator Fuel Transfer Pump	250	1 Hp	1-20	
Makeup Pump 3A Lube Oil Pump	250	1 Hp	0-20	
Makeup Pump 3B Lube Oil Pump	250	1 Hp	0-20	
Vacuum Breaker	250	.135 Hp	0-10	
Turbine Driven Emergency Feedwater Pump to Hotwell Isolation Valve	250	.09 Hp	10-11	
Auxiliary Feedwater Pump Turbine Steam Supply Isolation Valve	250	1.81 Hp	10-11	
Turbine Thrust Bearing Wear Detector Motor	125	.05 Hp	0-10	
EHC Cabinet	125	1 KVA	0-120	
Feedwater Pump Turbine Speed Changer	125	.166 Hp	0-10	
6900 Volt Switchgear 3A Control	125	*		3
4160 Volt Switchgear 3A Control	125	*		10
4160 Volt Engineered Safeguard Switchgear 3A Control	125	*		10
480 Volt Plant Auxiliary Bus 3 Control	125	*		-
480 Volt Reactor Auxiliary Bus 3A Control	125	*		2
480 Volt Turbine Auxiliary Bus 3A Control	125	*		7
480 Volt Heating Auxiliary Bus 3 Control	125	*		-
480 Volt Intake Auxiliary Bus 3A Control	125	*		4
480 Volt Engineered Safeguards Bus 3A Control	125	*		3
Inverter 3A	125	15 KVA	0-120	
Inverter 3C	125	15 KVA	0-120	
Condensate Demineralizer Control Panel	125	.625 KVA	0-120	
Instrument Repair Shop Receptacles	125	.625 KVA	0-120	
Engineered Safeguards Channel 3A Cabinets	125	.625 KVA	0-120	
Engineered Safeguards Actuation 3A Cabinets	125	.625 KVA	0-120	
Relay Racks	125	12.5 KVA	0-120	
Substation Loads	125	7.5 KVA	0-120	
Emergency Lighting	125	1.25 KVA	0-120	

*Power required to trip breakers as listed (10 amps/breaker for one minute).

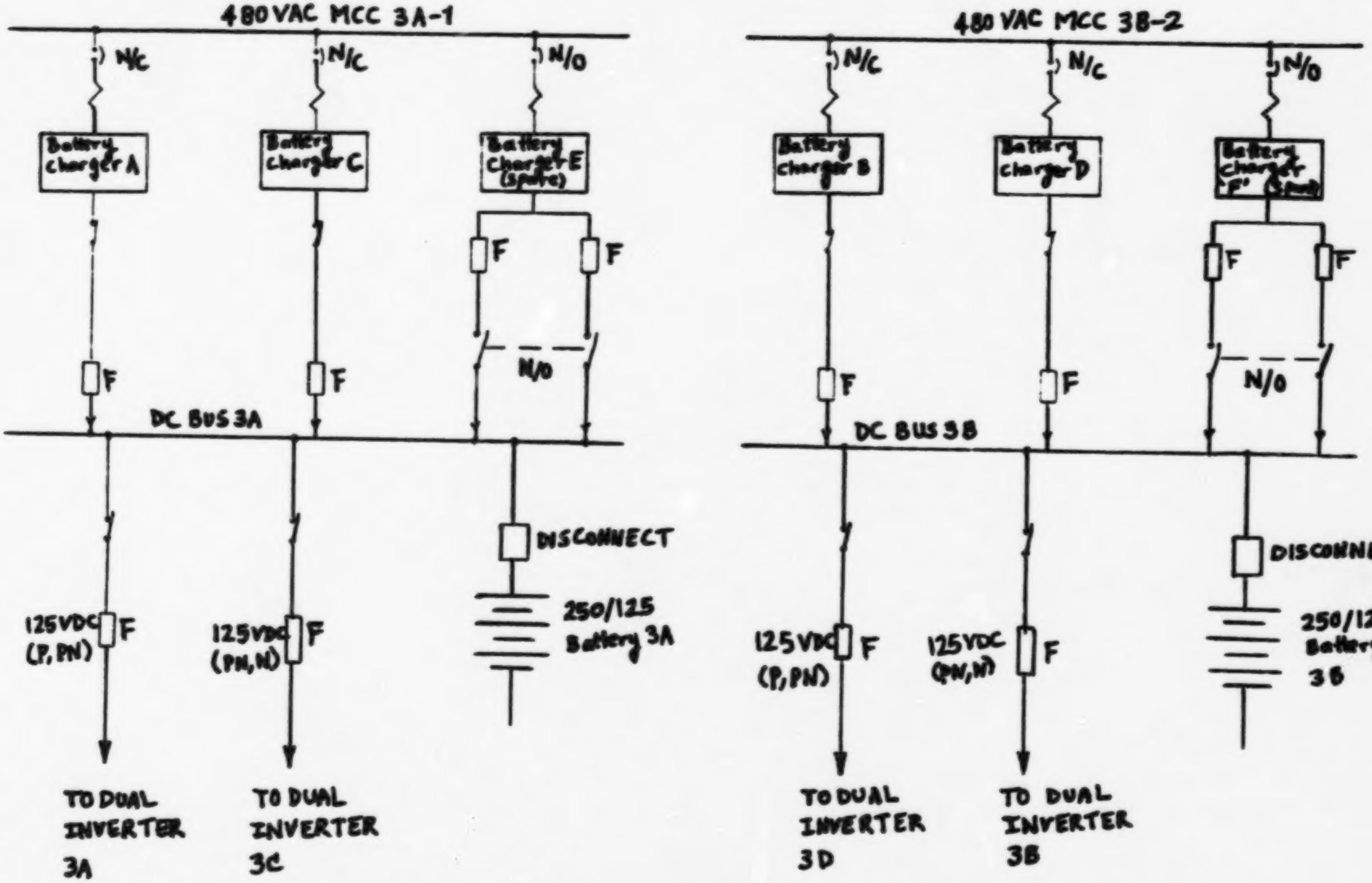

480 VAC MCC 3A-1
N/C
N/C
N/O
Battery charger A
Battery charger C
Battery Charger E (Spare)
F
F
F
F
N/O
DC BUS 3A
125VDC (P, PN)
F
125VDC (PN, N)
F
DISCONNECT
250/125 Battery 3A
TO DUAL INVERTER 3A
TO DUAL INVERTER 3C
480 VAC MCC 3B-2
N/C
N/C
N/O
Battery charger B
Battery charger D
Battery Charger 'F' (Spare)
F
F
F
F
N/O
DC BUS 3B
125 VDC (P, PN)
F
125VDC (PN, N)
F
DISCONNECT
250/125 Battery 3B
TO DUAL INVERTER 3D
TO DUAL INVERTER 3B

Figure C.1 DC Power System One Line Diagram

C.2 SYSTEM SIMPLIFIED FAULT TREE

The DCPS fault tree analysis consisted of developing trees which would serve as sub-trees (i.e., plug in modules) for the fault trees which were developed for the various systems that require DC power during normal plant operation and accident conditions including transients and loss of coolant accidents. Accordingly, fault trees were developed to identify the hardware and human failures which could inhibit the distribution of DC power from the individual DC panels to the associated systems.

TOP EVENT DEFINITION

The undesired event for which the DCPS fault trees were developed was:

"Insufficient Power at DC Panel DPDP-XX"

where: DPDP-XX represents the DC distribution panel associated with the particular system for which DC power was required.

ASSUMPTIONS

The underlying assumptions governing the development of the DCPS fault trees include:

1. Insufficient DC power is defined as loss of either of the 125VDC supplies provided by a 125VDC battery section and the associated charger.
2. Hardware failures, such as circuit breaker, switch or fuse failing open, are not immediately repairable. The failed hardware must be replaced in order to place the associated circuit back on-line.
3. The down time resulting from failures such as inadvertent switch opening or failure to re-close a switch is a function of detectability; i.e., DC system alarms and user equipment monitoring features.
4. Calibration failures such as mis-setting of one or more charges result in a down time after detection equal to the initial calibration period. Further, calibration errors are assumed detectable after associated equipment is placed on-line.

The simplified fault trees for the DCPS are presented in Figure C.2, sheets 1 through 15. Notes to the simplified fault trees are in Table C.3.

Table C.3 (1/4) Fault Tree Notes

GENERAL NOTES

(a) High and Low voltage alarm is provided in the control room for each of the six chargers employed for the two DC buses.

- o High alarm set point = 137VDC
- o Low alarm set point = 121VDC

(b) Reactor shall not be made critical unless both 250/125 volt DC supplies (bus 3A and 3B) are energized.

(c) During power operation one of the two 250/125 volt DC supplies may not be out of service for more than two hours.

(d) Charging current and load on each of the buses (3A&3B) are checked each shift.

(e) Battery discharge is monitored each shift by contact making ammeters located in each of the main DC panels (DPDP-1A&-1B).

(f) Voltage, specific gravity and electrolyte level of each battery cell are measured once each quarter. Pilot cells are checked weekly.

(g) Maintenance is performed on the batteries and chargers as required to correct for defects.

(h) During refueling each charger is demonstrated to be operable via an eight hour load test.

(i) Plant batteries are of the lead-calcium type.

Table C.3 (2/4) Fault Tree Notes

SPECIFIC NOTES

(1) Unless all equipment obtaining DC from a particular panel were on standby the likelihood is believed low that the panel input switch would be opened for maintenance on associated equipment. Most likely individual switches in the panel would be used to disable DC to equipment for maintenance.

(2) Those malfunctions would be immediately detected since operating systems would be disabled.

- If all equipment obtaining DC from the disabled panel are on standby then malfunction could go undetected until demand for the equipment occurred.
- Elapsed time to affect repairs depends on time to detect cause of DC loss and time to place switch in proper position.

(3) These malfunctions would have same effect as (2) above. A longer time would be required to affect repairs since failed hardware would have to be repaired or replaced.

(4) This malfunction causes loss of all DC from the associated 250/125VDC supply resulting in disabling of all equipment powered by this supply. Down time for the supply would be a function of time to detection and repair time.

Table C.3 (3/4) Fault Tree Notes

BATTERY CHARGER - NOTE 1

- Since work on a charger requires that it be disconnected from the DC bus, maintenance personnel may leave the switch, which disconnects charger from bus, in the "off" position. However, when work is being done on a charger a spare charger is switched on line. After work is completed the original charger might not be placed back on line even though spare charger has been disconnected.
- This condition can be discovered during daily check of charging voltage and/or charging current. During the time a battery is not on float charge, loads (DC) will be supplied directly by the battery (instead of by the charger) causing degradation in battery capability. This event will usually occur, if at all, during normal plant operation.

DC DISTRIBUTION PANELS

NOTES: 1. DC distribution panels consist of cabling and switches for applying DC to various user equipment. Maintenance personnel can inadvertently open a switch thereby removing the DC power from the associated user equipment.

2. If a particular component requires DC for its operation and Test and/or maintenance requires removal of DC power, maintenance personnel may fail to restore power.

Table C.3 (4/4) Fault Tree Notes

BATTERY

NOTE 1

- Batteries are housed in rooms requiring ventilation to prevent build-up of hydrogen which develops during float charging. Loss of ventilation can cause batteries to fail or degrade and possibly a significant (explosive) mixture of hydrogen can develop if charging continues after loss of ventilation.

NOTE 2

- During equalizing charge excess voltage may be applied. This can severely damage battery.
- During tests for grounds (system is ungrounded) all or part of the battery may be taken off line (momentarily).
- Too much electrolyte can be added.
- Cells may be "jumpered" for T&M and jumper may not be removed. This has the effects of degrading battery capability.

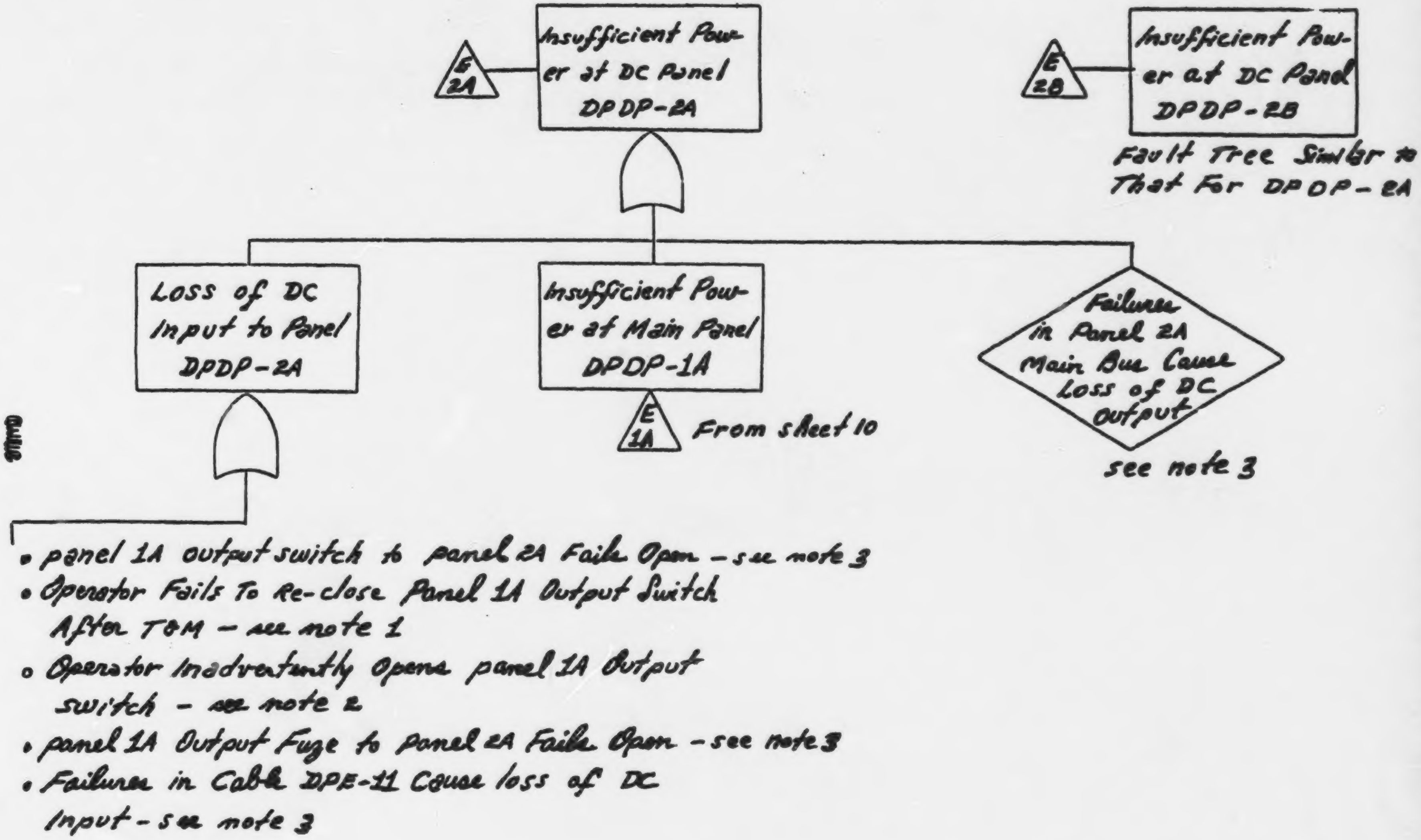
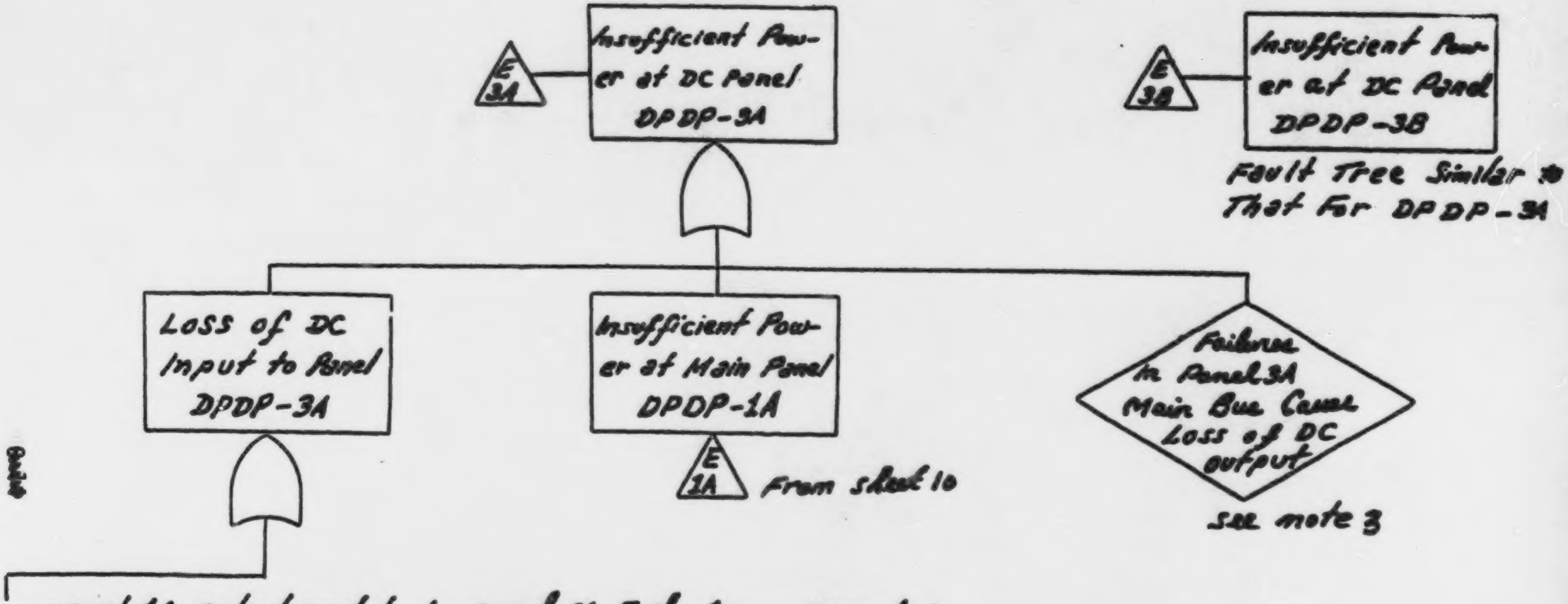
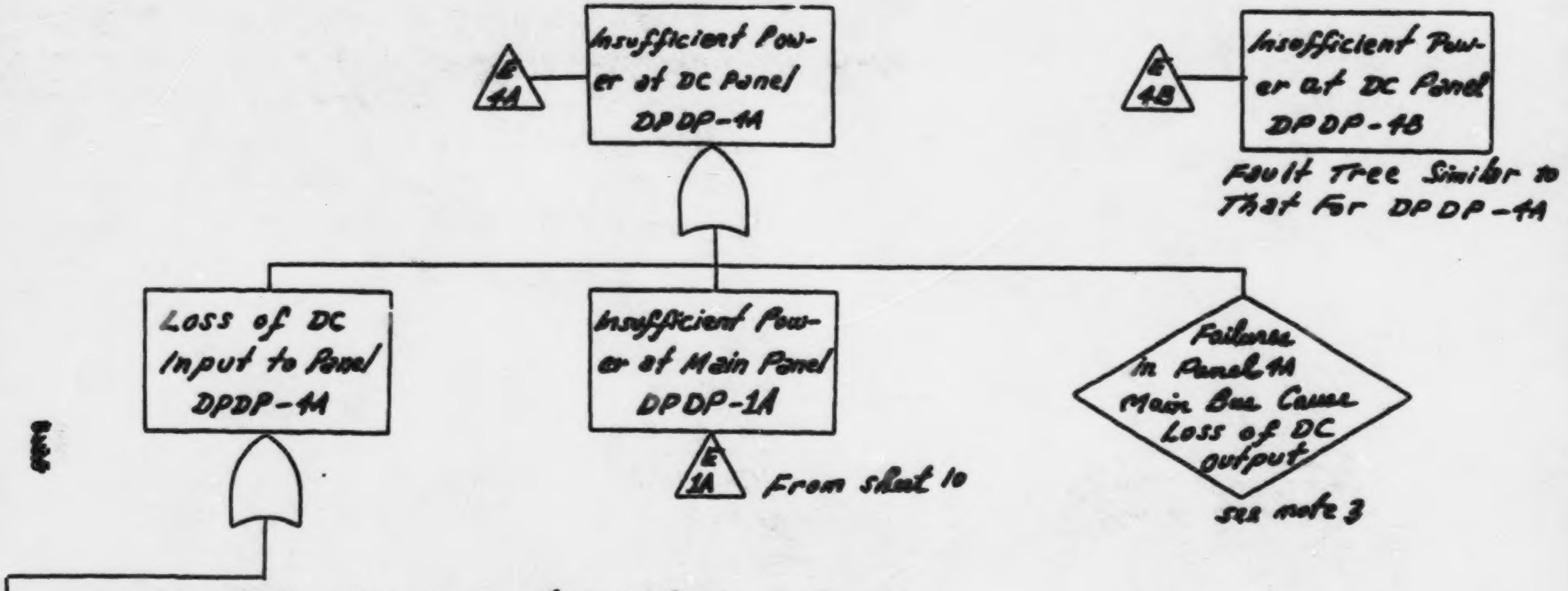

E 2A
Insufficient Power at DC Panel DPDP-2A
E 2B
Insufficient Power at DC Panel DPDP-2B
Fault Tree Similar to That For DPDP-2A
Loss of DC Input to Panel DPDP-2A
Insufficient Power at Main Panel DPDP-1A
E 1A
From sheet 10
Failures in Panel 2A Main Bus Cause Loss of DC Output
see note 3
• panel 1A output switch to panel 2A Fails Open - see note 3
• Operator Fails To Re-close Panel 1A Output Switch After T&M - see note 1
• Operator Inadvertently Opens panel 1A Output switch - see note 2
• panel 1A Output Fuze to panel 2A Fails Open - see note 3
• Failures in Cable DPE-11 Cause loss of DC Input - see note 3

Figure C.2 (1/15) Simplified Fault Tree DC Power System, Events "E2A" and "E2B"


E 3A
Insufficient Power at DC Panel DPDP-3A
E 3B
Insufficient Power at DC Panel DPDP-3B
Fault Tree Similar to That For DPDP-3A
Loss of DC Input to Panel DPDP-3A
Insufficient Power at Main Panel DPDP-1A
E 1A
From sheet 10
Failures in Panel 3A Main Bus Cause Loss of DC output
see note 3

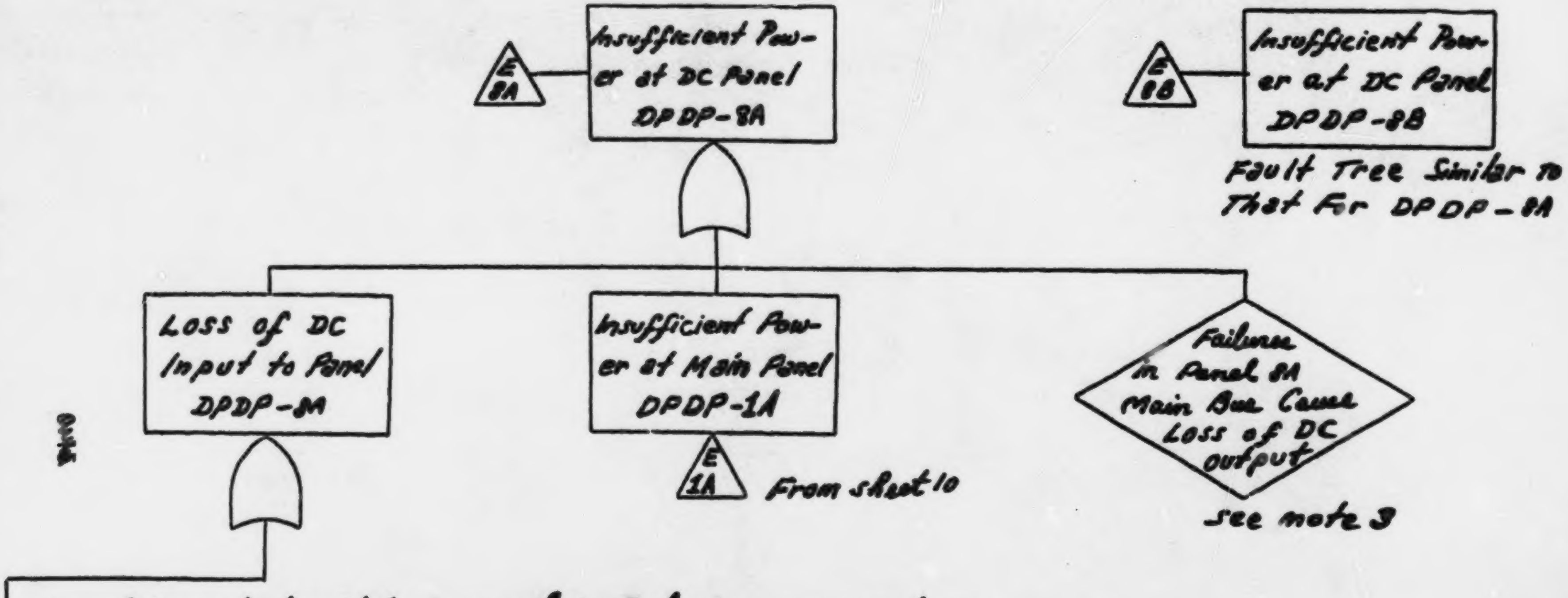
- panel 1A output switch to panel 3A Fails Open - see note 3
- Operator Fails To Re-close Panel 1A Output Switch After TGM - see note 1
- Operator Inadvertently Opens panel 1A Output switch - see note 2
- panel 1A Output Fuse to Panel 3A Fails Open - see note 3
- Failures in Cable DPE-10 Cause loss of DC Input - see note 3

Figure C.2 (2/15) Simplified Fault Tree DC Power System, Events "E3A" and "E3B"


E 4A
Insufficient Power at DC Panel DPDP-4A
E 4B
Insufficient Power at DC Panel DPDP-4B
Fault Tree Similar to That For DPDP-4A
Loss of DC Input to Panel DPDP-4A
Insufficient Power at Main Panel DPDP-1A
E 1A
From sheet 10
Failures in Panel 4A Main Bus Cause Loss of DC output
see note 3

- panel 1A output switch to panel 4A Fails Open - see note 3
- Operator Fails To Re-close Panel 1A Output Switch After T&M - see note 1
- Operator Inadvertently Opens panel 1A Output switch - see note 2
- panel 1A Output Fuse to panel 4A Fails Open - see note 3
- Failures in Cable DPE-17 Cause loss of DC Input - see note 3

Figure C.2 (3/15) Simplified Fault Tree DC Power System, Events "E4A" and "E4B"


E 8A
Insufficient Power at DC Panel DPDP-8A
E 8B
Insufficient Power at DC Panel DPDP-8B
Fault Tree Similar to That For DPDP-8A
Loss of DC Input to Panel DPDP-8A
Insufficient Power at Main Panel DPDP-1A
E 1A
From sheet 10
Failures in Panel 8A Main Bus Cause Loss of DC output
see note 3

- panel 1A Output switch to panel 8A Fails Open - see note 3
- Operator Fails To Re-close Panel 1A Output Switch After T&M - see note 1
- Operator Inadvertently Opens panel 1A Output switch - see note 2
- panel 1A Output Fuse to panel 8A Fails Open - see note 3
- Failures in Cable DPE-74 Cause loss of DC Input - see note 3

Figure C.2 (4/15) Simplified Fault Tree DC Power System, Events "E8A" and "E8B"

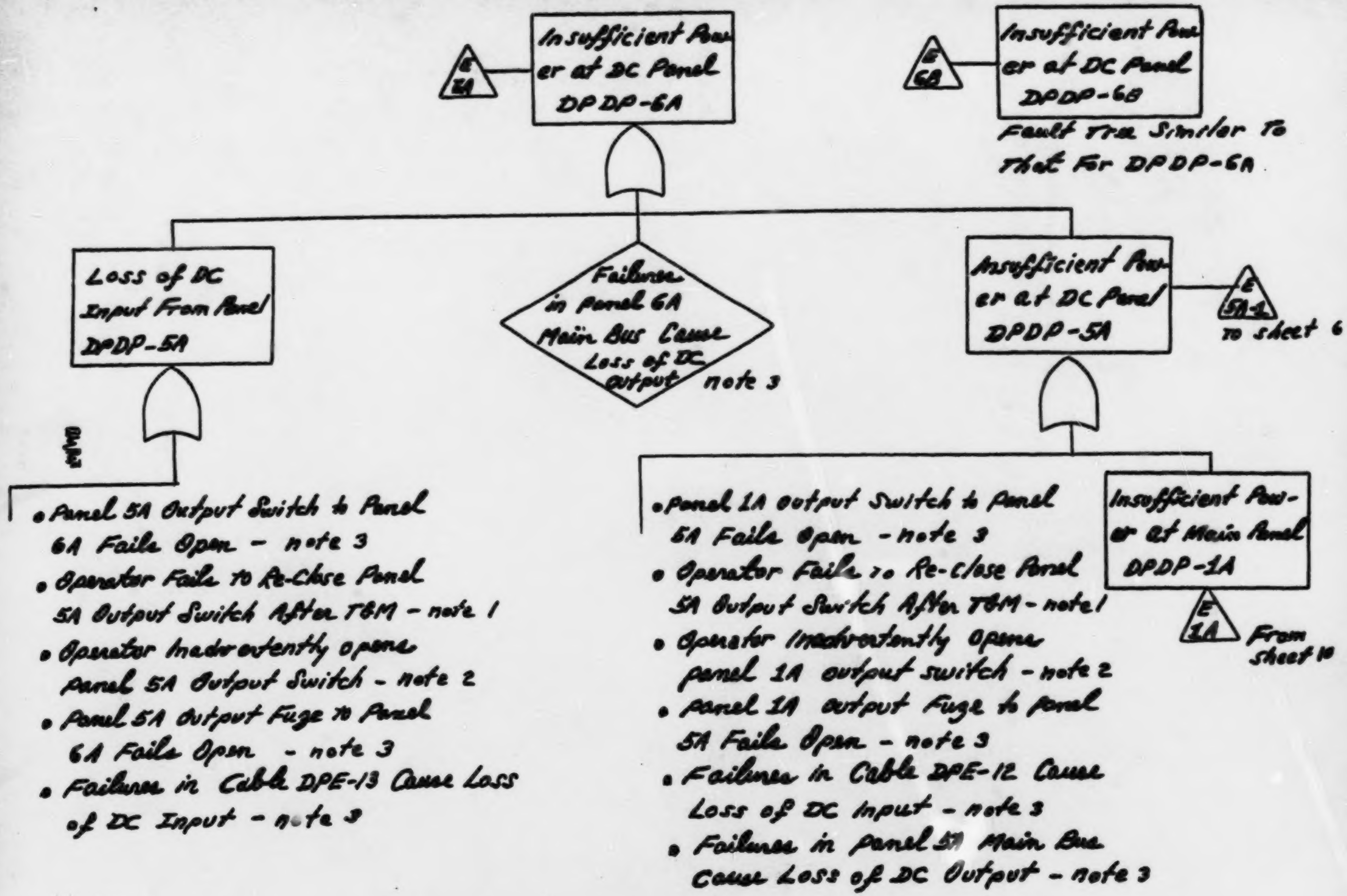

E 6A
Insufficient Power at DC Panel DPDP-6A
E 6B
Insufficient Power at DC Panel DPDP-6B
Fault Tree Similar To That For DPDP-6A
Loss of DC Input From Panel DPDP-5A
Failures in panel 6A Main Bus Cause Loss of DC output
note 3
Insufficient Power at DC Panel DPDP-5A
E 5A-1
To sheet 6
• Panel 5A Output Switch to Panel 6A Fails Open - note 3
• Operator Fails to Re-Close Panel 5A Output Switch After TBM - note 1
• Operator Inadvertently opens panel 5A Output Switch - note 2
• Panel 5A Output Fuse to Panel 6A Fails Open - note 3
• Failures in Cable DPE-13 Cause Loss of DC Input - note 3
• Panel 1A output Switch to Panel 5A Fails Open - note 3
• Operator Fails to Re-Close Panel 5A Output Switch After TBM - note 1
• Operator Inadvertently Opens panel 1A output switch - note 2
• Panel 1A output Fuse to Panel 5A Fails Open - note 3
• Failures in Cable DPE-12 Cause Loss of DC Input - note 3
• Failures in panel 5A Main Bus Cause Loss of DC Output - note 3
Insufficient Power at Main Panel DPDP-1A
E 1A
From sheet 10

Figure C.2 (5/15) Simplified Fault Tree DC Power System,
Events "E6A" and "E6B"

BEST DOCUMENT AVAILABLE

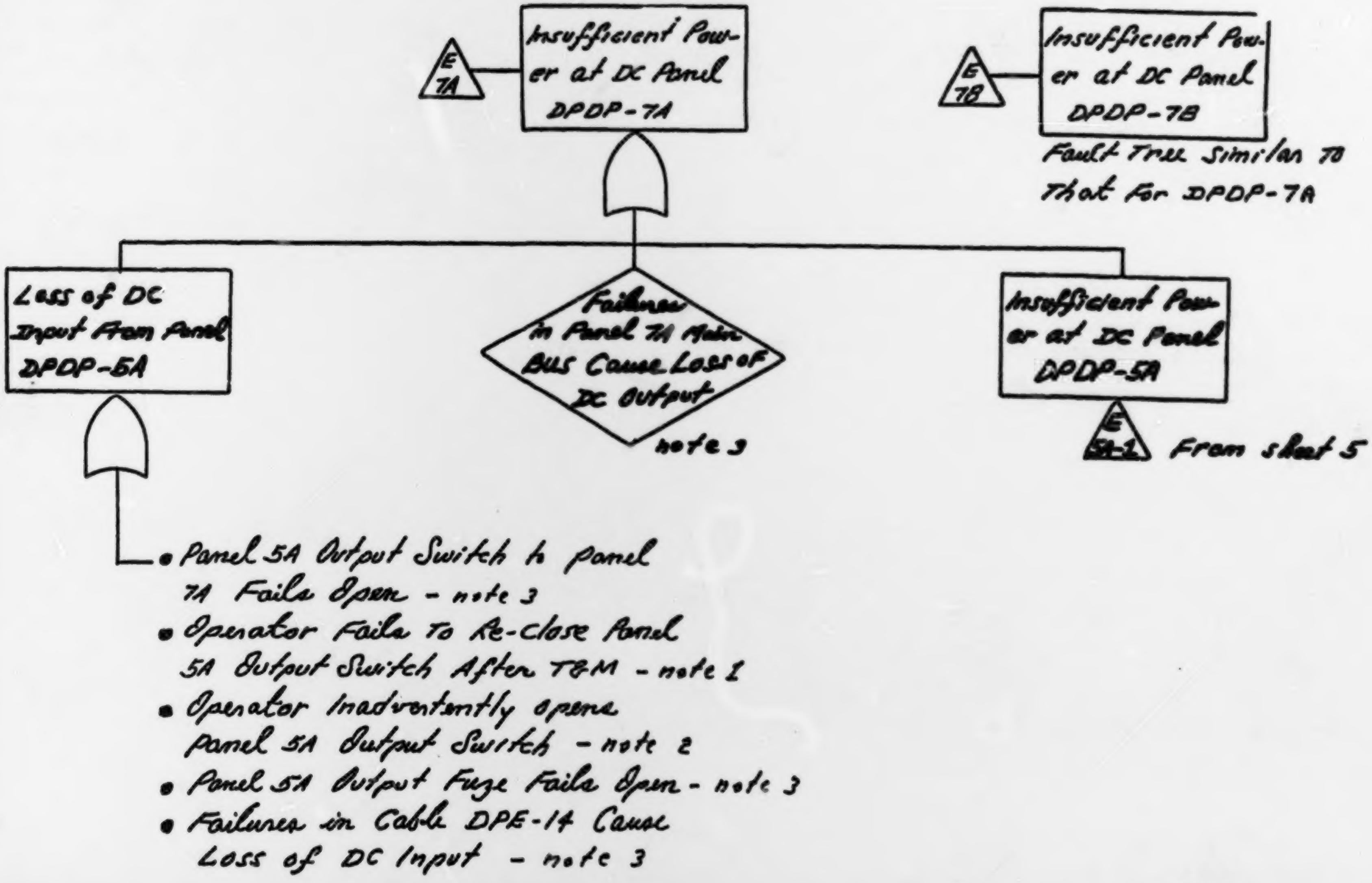

E 7A
Insufficient Power at DC Panel DPDP-7A
E 7B
Insufficient Power at DC Panel DPDP-7B
Fault Tree Similar To That For DPDP-7A
Loss of DC Input From Panel DPDP-5A
Failures in Panel 7A Main Bus Cause Loss of DC Output
note 3
Insufficient Power at DC Panel DPDP-5A
E 5A-1
From sheet 5
• Panel 5A Output Switch to panel 7A Fails Open - note 3
• Operator Fails To Re-Close Panel 5A Output Switch After T&M - note 1
• Operator Inadvertently opens Panel 5A Output Switch - note 2
• Panel 5A Output Fuze Fails Open - note 3
• Failures in Cable DPE-14 Cause Loss of DC Input - note 3

Figure C.2 (5115). Simplified Fault Tree DC Power System

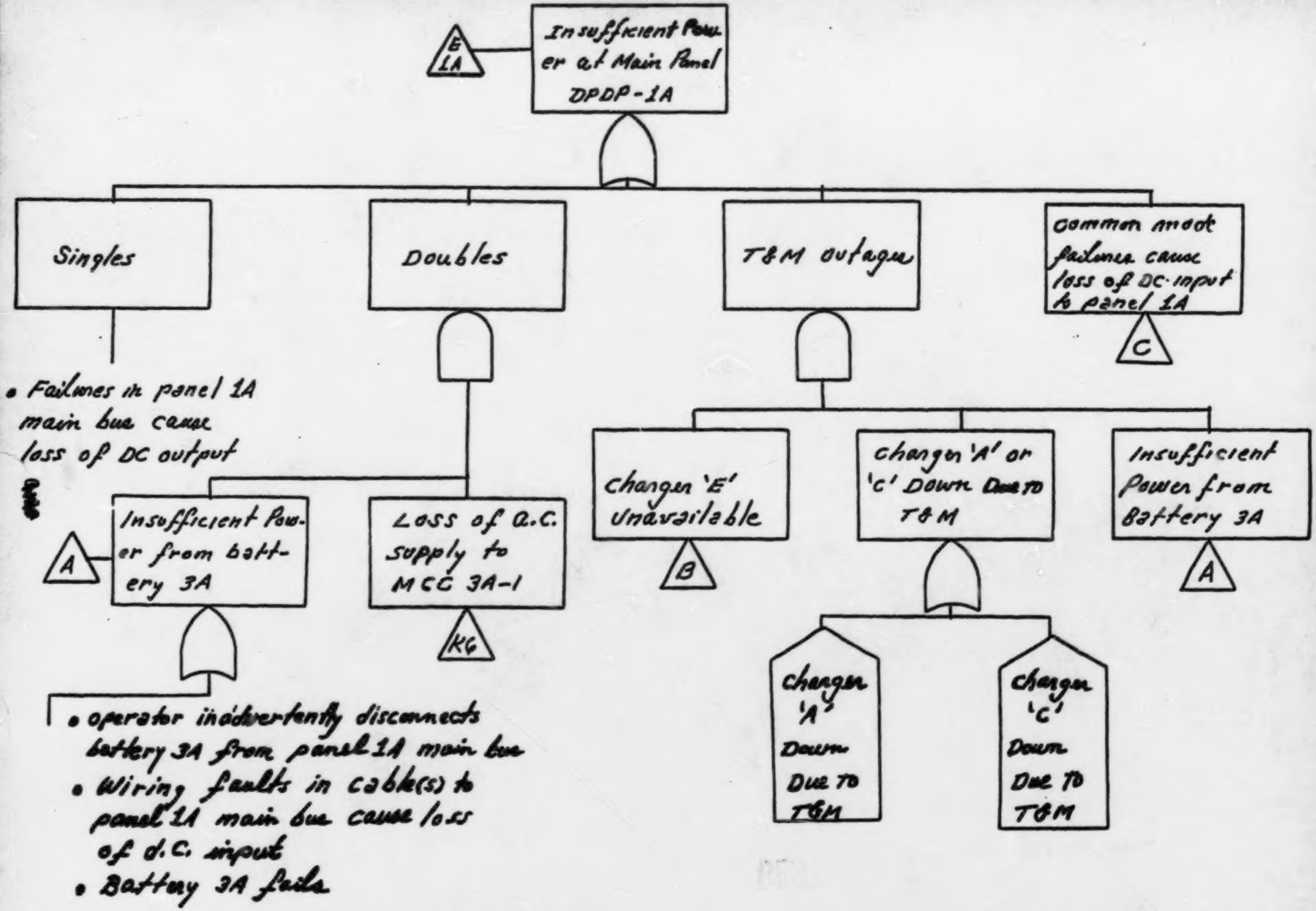
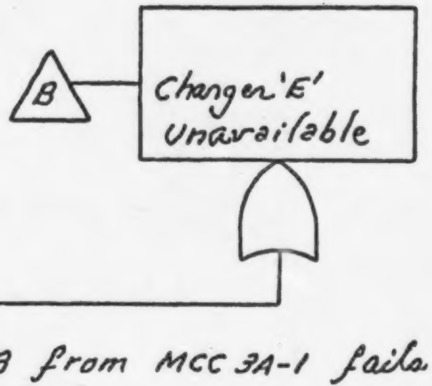

E 1A
Insufficient Power at Main Panel DPDP-1A
Singles
Doubles
T&M outage
common mode failures cause loss of DC input to panel 1A
C
• Failures in panel 1A main bus cause loss of DC output
Insufficient Power from battery 3A
A
Loss of a.c. supply to MCC 3A-1
K6
• operator inadvertently disconnects battery 3A from panel 1A main bus
• Wiring faults in cable(s) to panel 1A main bus cause loss of d.c. input
• Battery 3A fails
Charger 'E' Unavailable
B
Charger 'A' or 'C' Down Due To T&M
Insufficient Power from Battery 3A
A
Charger 'A' Down Due To T&M
Charger 'C' Down Due To T&M

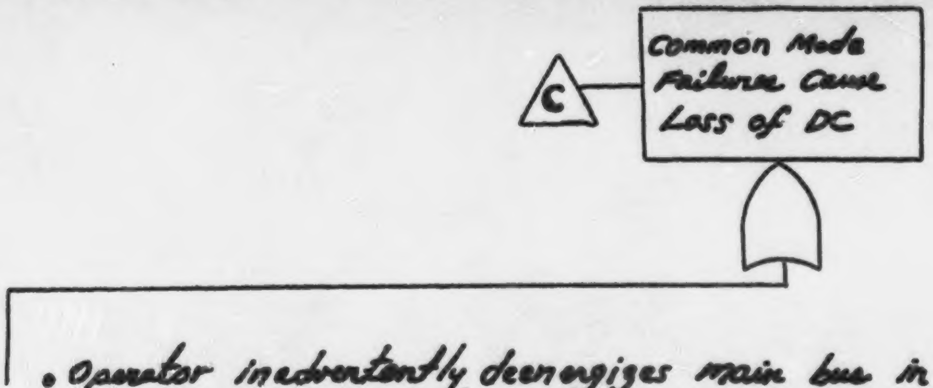
Figure C.2 (7/15) Simplified Fault Tree DC Power System, Event "E1A"

BEST DOCUMENT AVAILABLE



- Input CB from MCC 3A-1 fails open
- Charger fails
- panel 1A input switch to charger fails open
- panel 1A input fuze to charger fails open
- Failures in cable DPC-3 (input cable) cause loss of a.c. input
- Failures in cable DPE-9 (output cable) cause loss of d.c. output
- Operator fails to close panel 1A input switch to charger
- Incorrect charging level set by operator
  - Low level results in low bus voltage to battery section
  - high level results in charger trip-off

Figure C.2 (8/15) Simplified Fault Tree DC Power System, Event "B"



- Operator inadvertently deenergizes main bus in panel 1A
- Loss of d.c. due to low charging level - Low voltage on main bus in Panel 1A
  - Low Charging Level on all Chargers set by Operator
  - Low battery voltage due to low charging level
  - Low charging level (voltage and current) monitored
- Loss of d.c. due to high charging level - No d.c. on main bus in panel 1A
  - High Charging Level on all chargers set by operator
  - Battery fails due to high charging level
  - High charging level (voltage and current) monitored
  - Chargers trip off due to high charging level
- Loss of d.c. due to ventilation system failure
  - Battery failure due to loss of ventilation
  - Chargers trip off due to battery overload
  - ventilation and battery failure undetected before charger trip-off
- Common mode piece-part, material, design or manufacturing defects cause all chargers or battery to fail
  - Battery failure causes charger trip-off due to overload
  - Charger failure causes battery damage

Figure C.2 (9/15) Simplified Fault Tree DC Power System, Event "C"

BEST DOCUMENT AVAILABLE

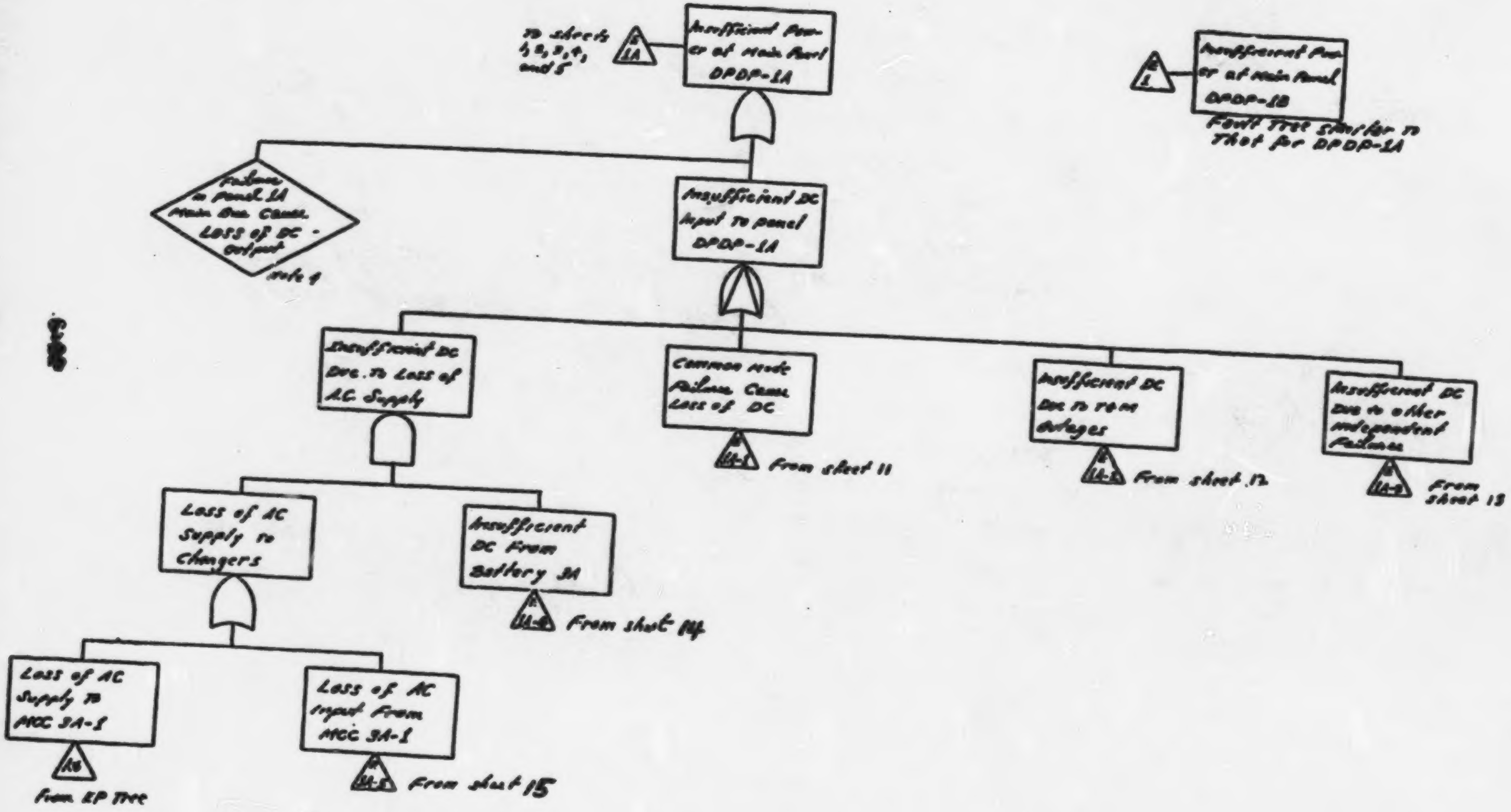
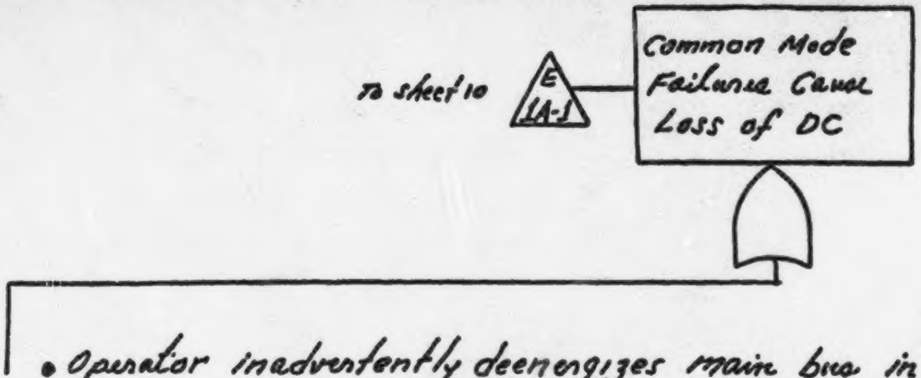
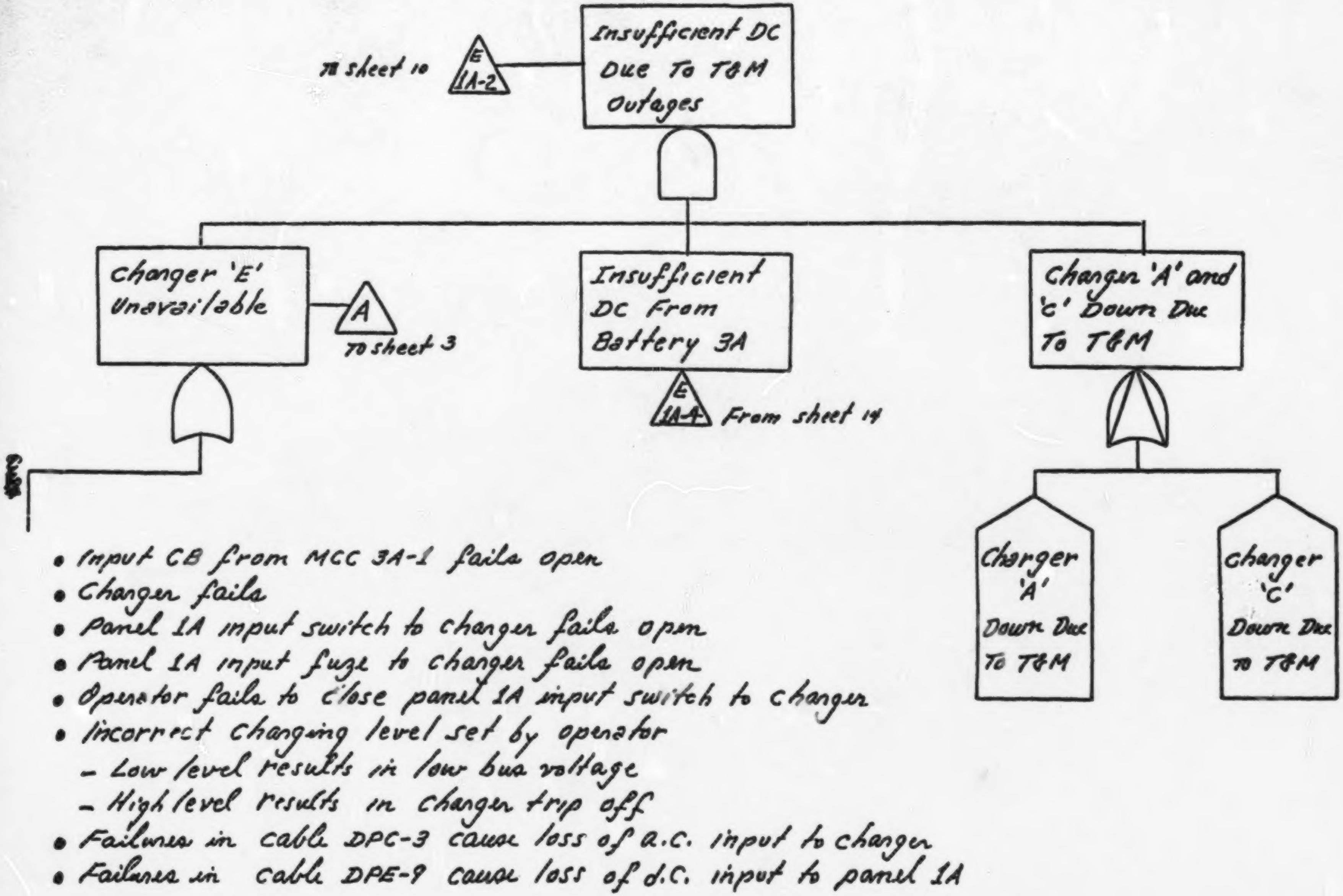

To sheets 1, 2, 3, 4, and 5
E 1A
Insufficient Power at Main Panel DPDP-1A
E 1
Insufficient Power at Main Panel DPDP-1B
Fault Tree similar to That for DPDP-1A
Failure in Panel 1A Main Bus Causes LOSS of DC - Output
note 4
Insufficient DC Input to panel DPDP-1A
Insufficient DC Due to Loss of AC Supply
Common Mode Failure Cause Loss of DC
E 1A-1
From sheet 11
Insufficient DC Due to T&M Outages
E 1A-2
From sheet 12
Insufficient DC Due to other independent Failures
E 1A-3
From sheet 13
Loss of AC Supply to Chargers
Insufficient DC From Battery 3A
E 1A-4
From sheet 14
Loss of AC Supply to MCC 3A-1
R6
From EP Tree
Loss of AC Input From MCC 3A-1
E 1A-5
From sheet 15

Figure C.2 (10/15) Simplified Fault Tree DC Power System,



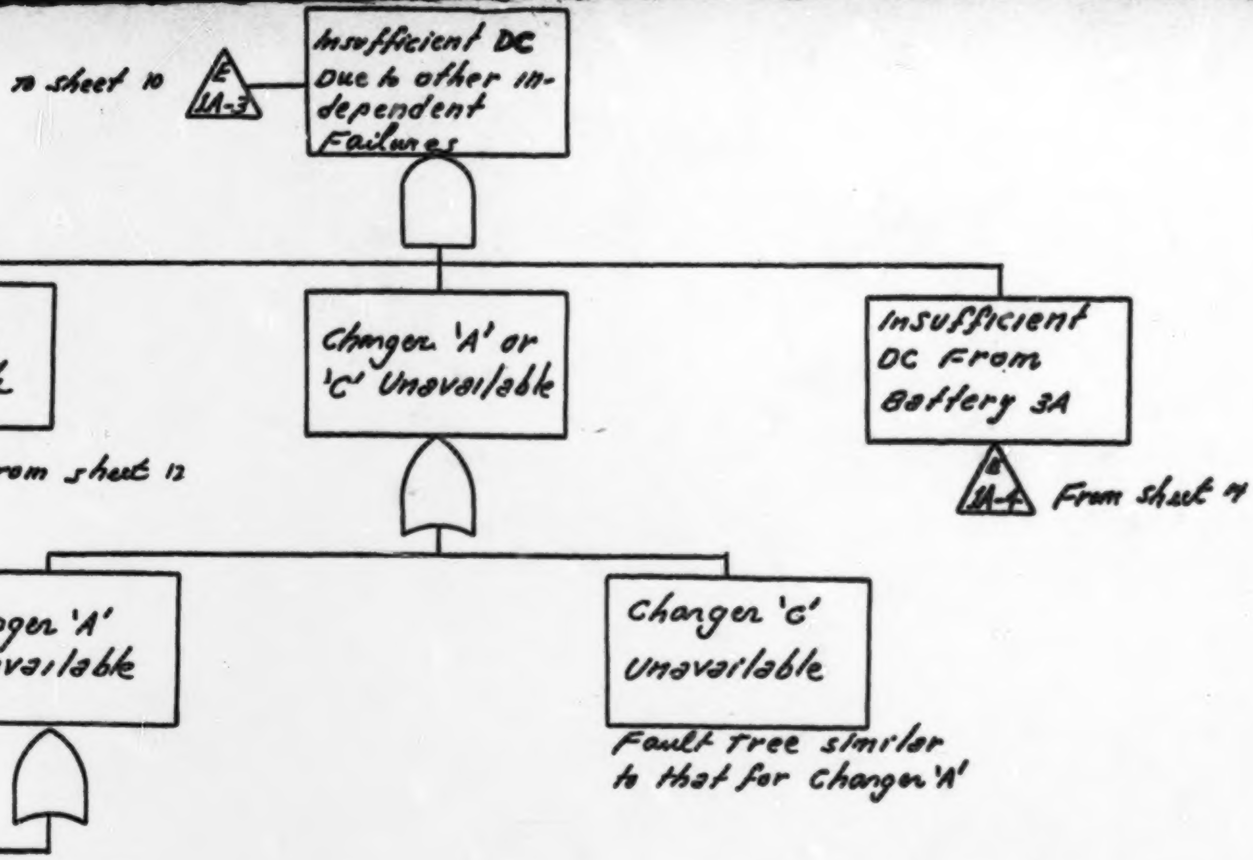
- Operator inadvertently deenergizes main bus in panel 1A
- Loss of d.c. due to low charging level - Low voltage on main bus in panel 1A
  - Low Charging Level on all chargers set by Operator
  - Low battery voltage due to low charging level
  - Low charging level (voltage and current) monitored
- Loss of d.c. due to high charging level - No d.c. on main bus in panel 1A
  - High Charging Level on all chargers set by operator
  - Battery fails due to high charging level
  - High charging level (voltage and current) monitored
  - Chargers trip off due to high charging level
- Loss of d.c. due to ventilation system failure
  - Battery failure due to loss of ventilation
  - Chargers trip off due to battery overload
  - ventilation and battery failure undetected before charger trip-off
- Common mode piece-part, material, design or manufacturing defects cause all chargers or battery to fail
  - Battery failure causes charger trip-off due to overload
  - Charger failure causes battery damage

Figure C.2 (11/15) Simplified Fault Tree DC Power System, Event "E1A-1"


Insufficient DC Due To T&M Outages
To sheet 10
E 1A-2
Charger 'E' Unavailable
A
To sheet 3
Insufficient DC From Battery 3A
E 1A-4
From sheet 14
Charger 'A' and 'C' Down Due To T&M
Charger 'A' Down Due To T&M
Charger 'C' Down Due To T&M

- Input CB from MCC 3A-1 fails open
- Charger fails
- Panel 1A input switch to charger fails open
- Panel 1A input fuze to charger fails open
- Operator fails to close panel 1A input switch to charger
- Incorrect charging level set by operator
  - Low level results in low bus voltage
  - High level results in charger trip off
- Failures in cable DPC-3 cause loss of a.c. input to charger
- Failures in cable DPE-9 cause loss of d.c. input to panel 1A

Figure C.2 (12/15) Simplified Fault Tree DC Power System, Event "E1A-2"


To sheet 10
E
1A-3
Insufficient DC Due to other independent Failures
Charger 'E' Unavailable
A
From sheet 12
Charger 'A' or 'C' Unavailable
Insufficient DC From Battery 3A
B
1A-4
From sheet 14
Charger 'A' Unavailable
Charger 'C' Unavailable
Fault Tree similar to that for Charger 'A'

- Input CB from MCC 3A-1 fails open
- Charger fails
- Panel 1A input switch to charger fails open
- Panel 1A input fuze to charger fails open
- Operator fails to re-close input CB or panel 1A input switch after T&M
- Operator inadvertently opens input CB or panel 1A input switch
- Incorrect charging level set by operator
  - low level results in low bus voltage
  - high level results in charger trip-off

- Failures in cable DPC-1 cause loss of a.c. input to charger
- Failures in cable DPE-7 cause loss of d.c. output to panel 1A

Figure C.2 (13/15) Simplified Fault Tree DC Power System, Event "E1A-3"

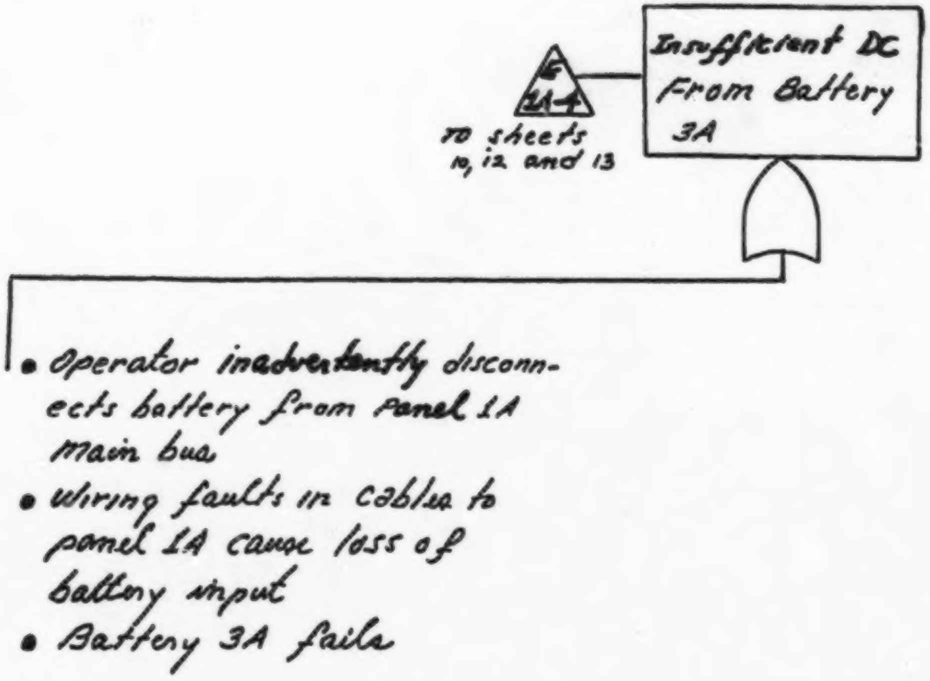
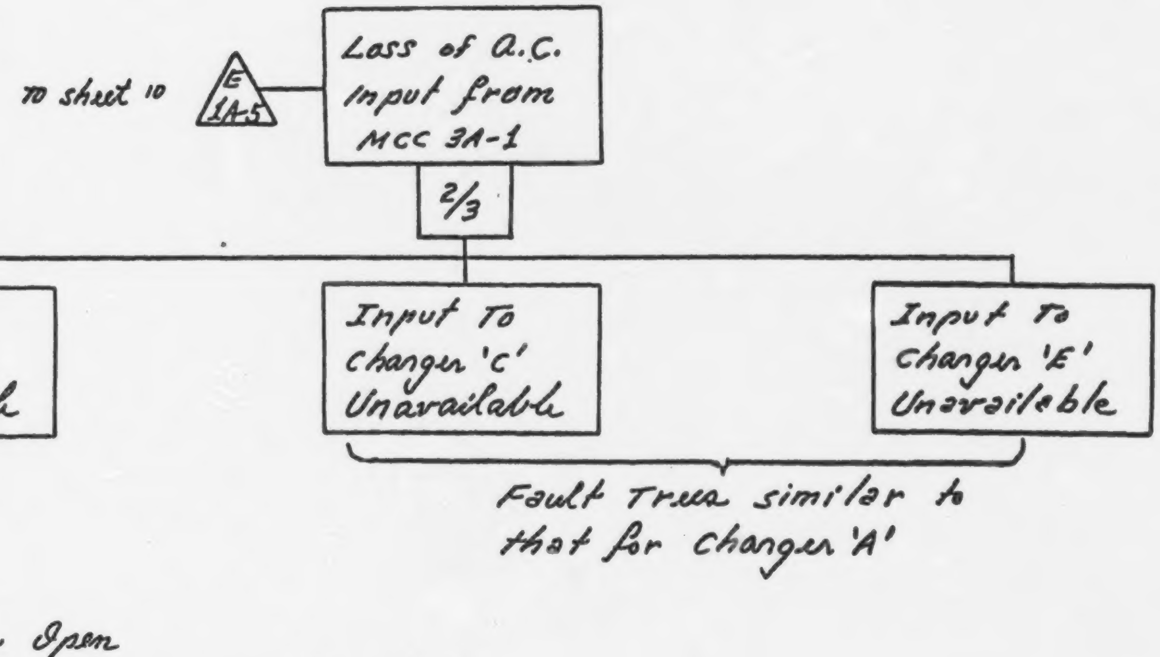

E1A-4
TO sheets 10, 12 and 13
Insufficient DC From Battery 3A
• Operator inadvertently disconnects battery from Panel 1A main bus
• Wiring faults in cables to panel 1A cause loss of battery input
• Battery 3A fails

Figure C.2 (14/15) Simplified Fault Tree DC Power System, Event "E1A-4"


To sheet 10
E
1A-5
Loss of A.C.
Input from
MCC 3A-1
2/3
Input To
Changer 'A'
Unavailable
Input To
Changer 'C'
Unavailable
Input To
Changer 'E'
Unavailable
Fault Trees similar to
that for Changer 'A'

- Input CB fails Open
- Operator inadvertently opens input CB
- Operator fails to re-close input CB After T&M on Changer
- Failures in cable DPC-1 Cause loss of A.C. input to Changer

Figure C.2 (15/15) Simplified Fault Tree DC Power System, Event "E1A-5"

C.3 SYSTEM QUANTIFICATION

C.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The DC Power Distribution System is a two train system consisting of independent batteries, battery chargers and buses. DC power is normally supplied by the independent battery chargers. A third battery charger can be manually switched to either train should one of the chargers normally in operation be removed from service. The battery chargers are normally driven by AC power. Should an AC power train be lost resulting in the loss of one charger, the battery assumes the DC loads on that train.

The battery charger voltage and battery internal current are normally monitored. Each DC bus was assumed to be effectively monitored, since loss of DC voltage at a bus would result in the loss of instrumentation that is normally operational, and it was assumed that this would be detected by the operators. Thus, during normal operation the DC system was assumed to be monitored.

For the case where offsite power is available, the unavailability of each DC bus was assessed based on a two hour bus outage time allowed by Technical Specifications. The unavailability in this case was small, and assessed to be primarily due to loss of a fuse.

For the loss of offsite power case, the unavailability of all buses on a single train is dominated by failure of the battery supplying that train. Since the battery is also required for the corresponding train of AC power, failure of a battery would fail one train of DC power and the corresponding train of AC power (see AC power fault tree quantification tables).

The failure of the DC power distribution system during the recirculation phase of a postulated accident was evaluated to be negligible for both the cases where offsite power is available or lost, since offsite power is assumed to be recovered by this phase.

C.3.2 SYSTEM FAULT TREE QUANTIFICATION

This section presents the quantification of the DC power system unavailability for required emergency operation. The quantitative results are presented in table form with attached notes outlining the assumptions. To perform the quantification, the simplified fault tree presented in Section E.2 was rearranged and is presented in this section in modular form.

Modularized fault trees were constructed for each DC bus for the case where offsite power is available. For the case where offsite power is lost, a single fault tree was constructed for the DC power system, since the dominant faults are loss of the batteries, which fail all buses.

Table C.4 shows the DC power success requirements, Table C.5 contains the top event definition for the modularized fault trees, and Figures C.4 through C.12 show the modularized fault trees. The unavailability of each gate is shown on these trees, as well as the top event unavailabilities. Table C.6 shows the Boolean equations that represent each fault tree. Table C.7, the quantification table, shows the quantification of each gate by component and failure mode. The attached notes explain the assumptions used in the quantification. Table C.8 summarizes the point estimates for each gate, and the error factors that were used in the sensitivity analysis.

Table C.4 DC Power Success Requirements

INITIATOR	TRAINS	NOTES
All	DC power on all DC buses	1

NOTES: 1. Failure of any DC bus would fail instrumentation and circuit breaker's power from that bus.

Table C.5 DC Power Top-Event Definitions*

BOOLEAN REPRESENTATION	TOP EVENTS	NOTES
Non-LOSP Case		
DPDP-1A (1B)	Insufficient power on bus DPDP-1A (1B)	1
DPDP-2A (2B)	" " " " DPDP-2A (2B)	2
DPDP-3A (3B)	" " " " DPDP-3A (3B)	2
DPDP-8A (8B)	" " " " DPDP-8A (8B)	2
DPDP-4A (4B)	" " " " DPDP-4A (4B)	2
BC-3A (3B)	" " " " BC-3A (3B)	2
BC-3C (3D)	" " " " BC-3C (3D)	2
BC-3E (3F)	" " " " BC-3E (3F)	2
DPDP-5A (5B)	" " " " DPDP-5A (5B)	2
DPDP-6A (6B)	" " " " DPDP-6A (6B)	3
DPDP-7A (7B)	" " " " DPDP-7A (7B)	3
Loss of Offsite Power Case		
DCA	Insufficient power on DC Train A buses	4
DCB	" " " " " B "	5
DC	Loss of both trains of DC power	6

---

*See Figure C.3 for bus dependencies.

Table C.5 DC Power

TOP EVENT DEFINITIONS

NOTES

1 DC - buses DPDP-1A and DPDP-1B are the main DC-panels for the A- and B-trains of DC-power. All other buses are connected to these.

2 These buses are connected directly to the main DC-power buses.

3 DPDP-6A and 7A are connected to subpanel DPDP-5A. DPDP-6B and -7B are connected to subpanel DPDP-5B.

4 This top event is evaluated for loss of all buses on DC-Train A.

5 This top event is evaluated for loss of all buses on DC-Train B.

6 This top event represents loss of all DC-power.

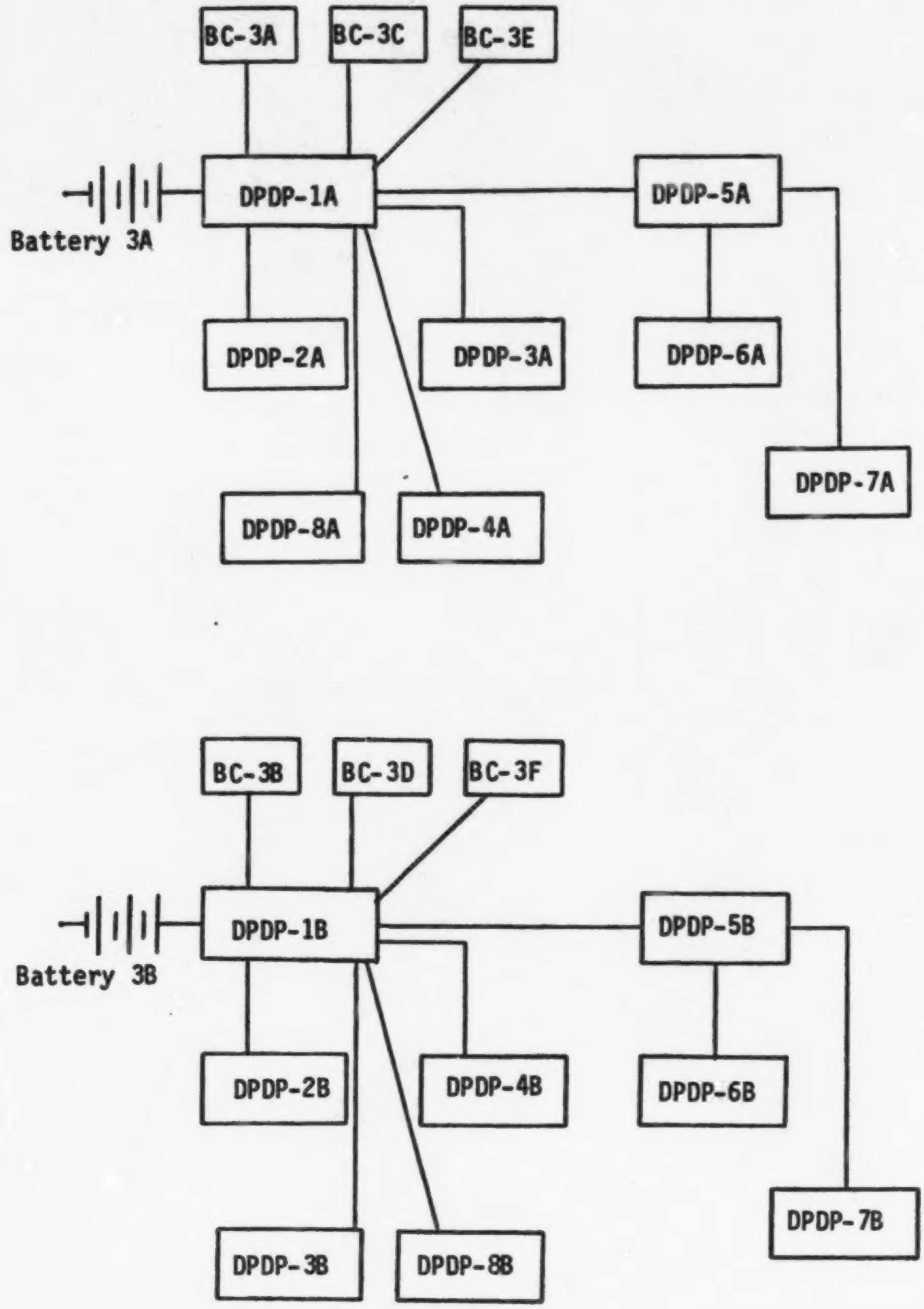

BC-3A
BC-3C
BC-3E
DPDP-1A
Battery 3A
DPDP-5A
DPDP-2A
DPDP-3A
DPDP-6A
DPDP-7A
DPDP-8A
DPDP-4A
BC-3B
BC-3D
BC-3F
DPDP-1B
Battery 3B
DPDP-5B
DPDP-2B
DPDP-4B
DPDP-6B
DPDP-7B
DPDP-3B
DPDP-8B

Figure C.3 DC Power - Bus Dependencies

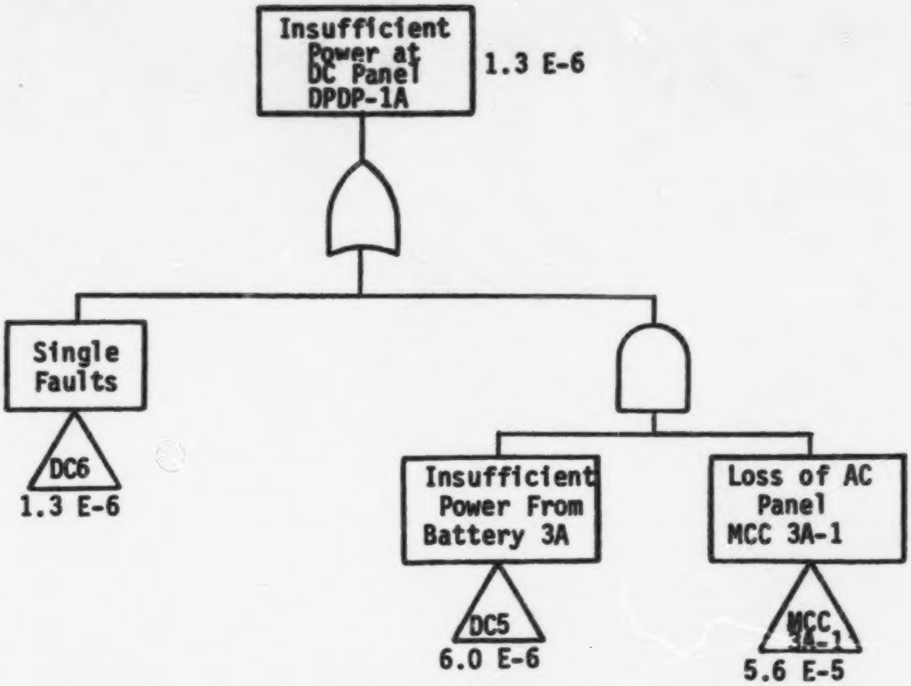

Insufficient Power at DC Panel DPDP-1A
1.3 E-6
Single Faults
DC6
1.3 E-6
Insufficient Power From Battery 3A
DC5
6.0 E-6
Loss of AC Panel MCC 3A-1
MCC 3A-1
5.6 E-5

Figure C.4 Modularized Fault Tree for Event "DPDP-1A" (Non-LOSP)

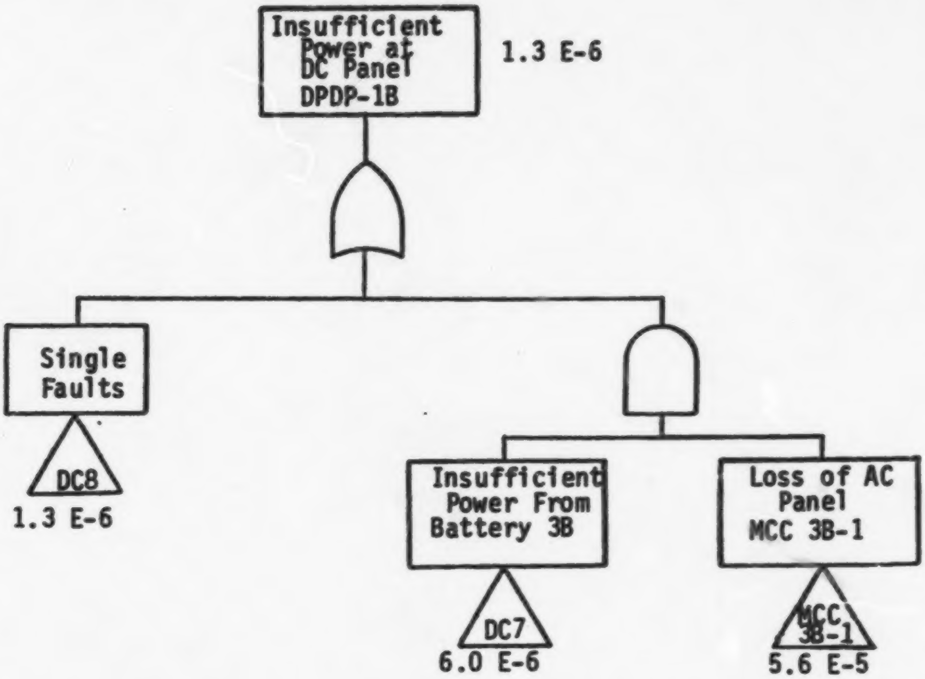

Insufficient Power at DC Panel DPDP-1B
1.3 E-6
Single Faults
DC8
1.3 E-6
Insufficient Power From Battery 3B
DC7
6.0 E-6
Loss of AC Panel MCC 3B-1
MCC 3B-1
5.6 E-5

Figure C.5 Modularized Fault Tree for Event "DPDP-1B" (Non-LOSP)

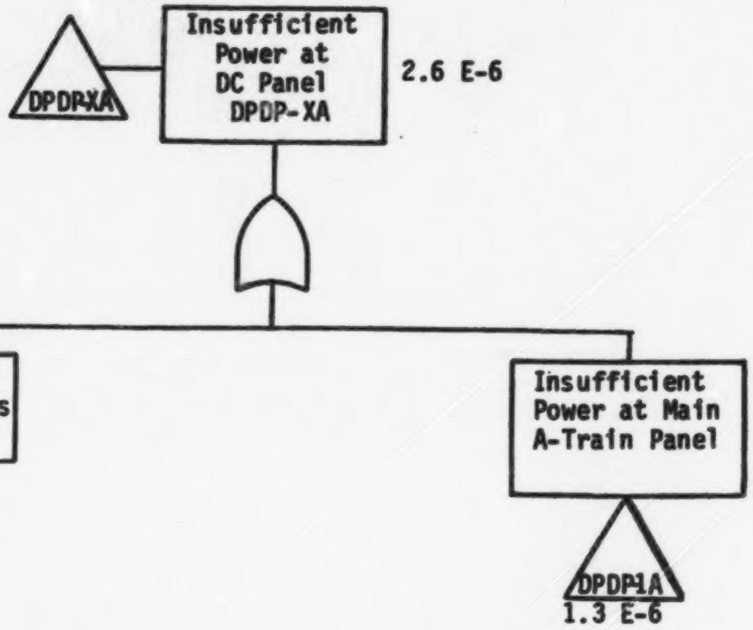

DPDP-XA
Insufficient Power at DC Panel DPDP-XA
2.6 E-6
Single Faults
DC1X
1.3 E-6
Insufficient Power at Main A-Train Panel
DPDP1A
1.3 E-6

Figure C.6 Modularized Fault Tree for Event "DPDP-XA"
(X = 2,3,4,5,8; Non-LOSP)

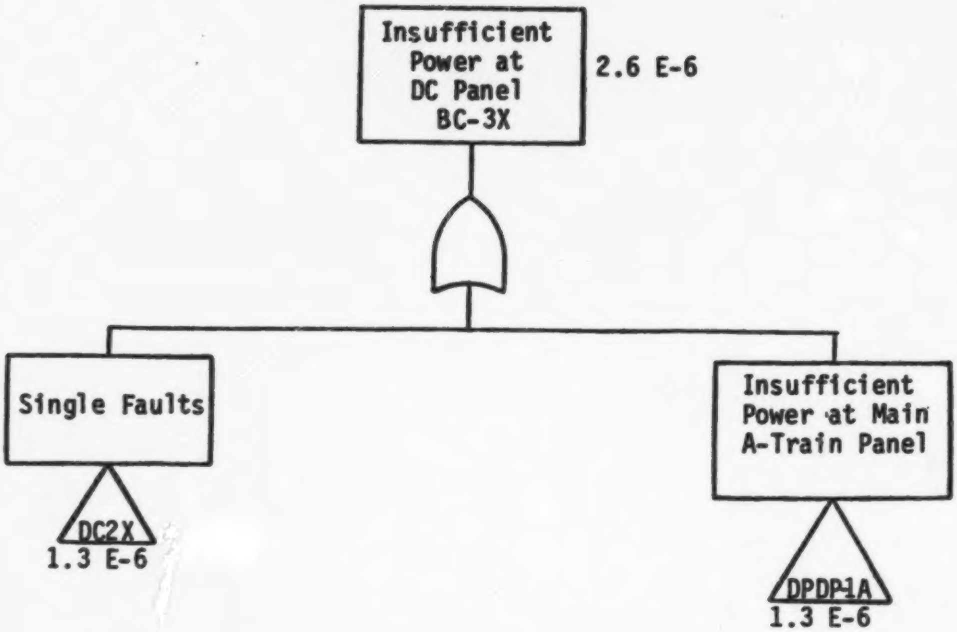

Insufficient Power at DC Panel BC-3X
2.6 E-6
Single Faults
DC2X
1.3 E-6
Insufficient Power at Main A-Train Panel
DPDP1A
1.3 E-6

Figure C.7 Modularized Fault Tree for Event "BC-3X"
(X = A,C.E; Non-LOSP)

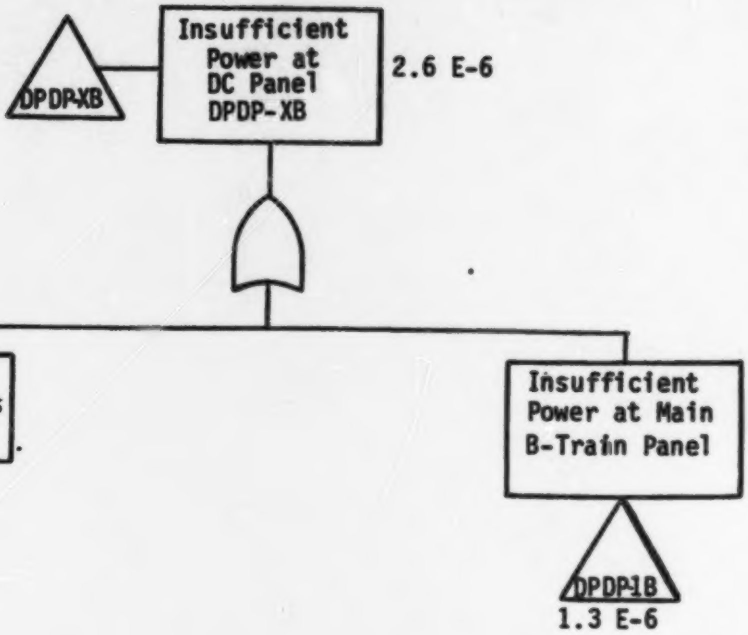

DPDP-XB
Insufficient Power at DC Panel DPDP-XB
2.6 E-6
Single Faults
DC3X
1.3 E-6
Insufficient Power at Main B-Train Panel
DPDP1B
1.3 E-6

Figure C.8 Modularized Fault Tree for Event "DPDP-XB"
(X = 2,3,4,5,8; Non-LOSP)

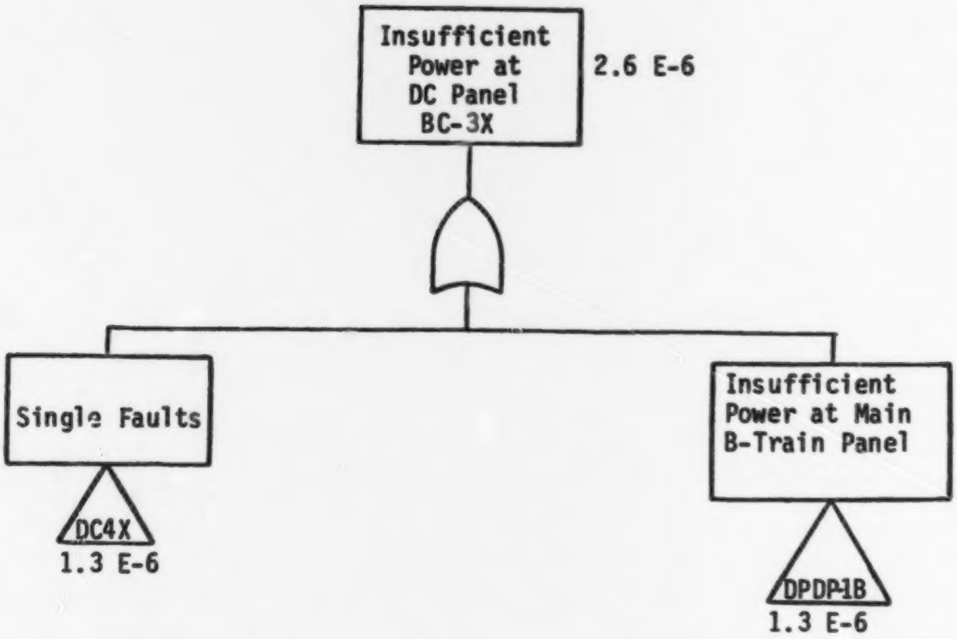

Insufficient Power at DC Panel BC-3X
2.6 E-6
Single Faults
DC4X
1.3 E-6
Insufficient Power at Main B-Train Panel
DPDP1B
1.3 E-6

Figure C.9 Modularized Fault Tree for Event "BC-3X"
(X = B,D,F; Non-LOSP)

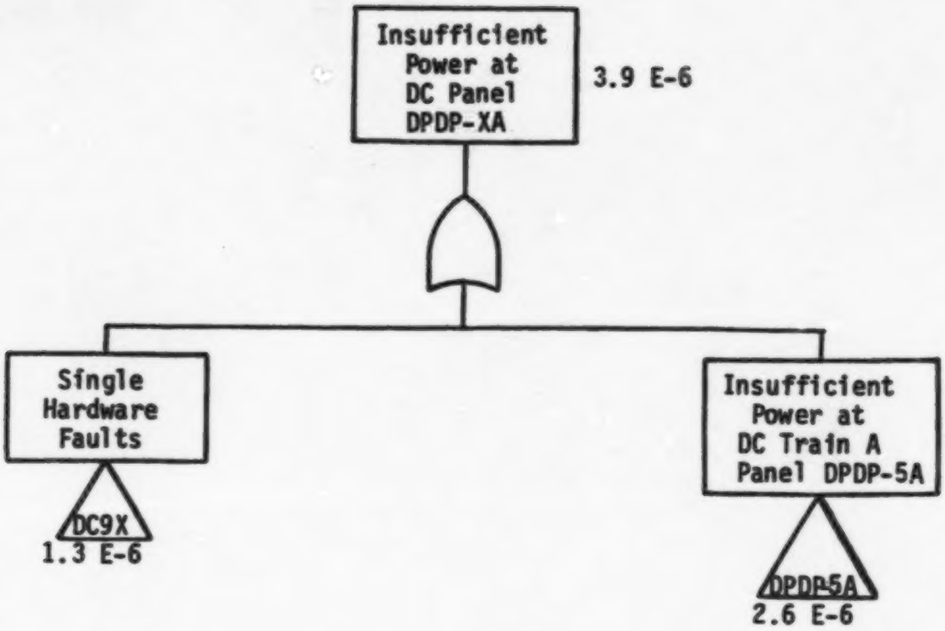

Insufficient Power at DC Panel DPDP-XA
3.9 E-6
Single Hardware Faults
DC9X
1.3 E-6
Insufficient Power at DC Train A Panel DPDP-5A
DPDP5A
2.6 E-6

Figure C.10 Modularized Fault Tree for Event "DPDP-XA" (X = 6,7; Non-LOSP)

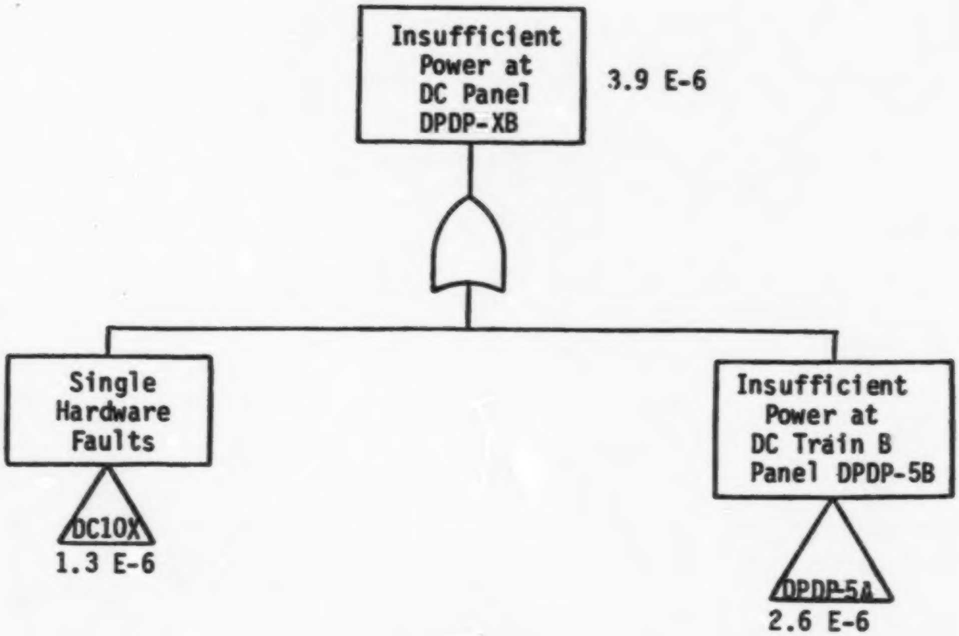

Insufficient Power at DC Panel DPDP-XB
3.9 E-6
Single Hardware Faults
DC10X
1.3 E-6
Insufficient Power at DC Train B Panel DPDP-5B
DPDP-5A
2.6 E-6

Figure C.11 Modularized Fault Tree for Event "DPDP-XB" (X = 6,7,; Non-LOSP)

[illegible]

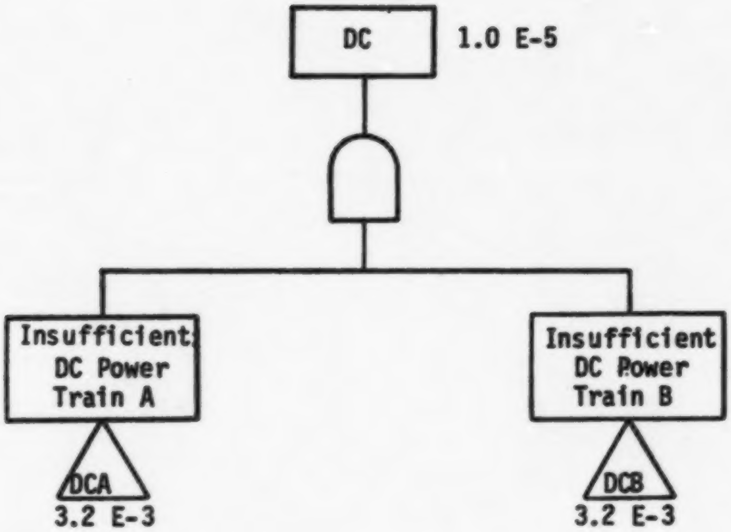

DC
1.0 E-5
Insufficient DC Power Train A
Insufficient DC Power Train B
DCA
3.2 E-3
DCB
3.2 E-3

Figure C.12 Modularized Fault Tree for Event "DC" (LOSP)

Table C.6 DC Power

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS

NON-LOSP

DPDP-XA = DC1X + DPDP-1A   X = 2,3,4,5,8
BC-3X = DC2X + DPDP-1A   X = A,C,E
DPDP-XB = DC3X + DPDP-1B   X = 2,3,4,5,8
BC-3X = DC4X + DPDP-1B   X = B,D,F
DPDP-1A = DC6 + DC5·MCC3A-1
DPDP-1B = DC8 + DC7·MCC3B-1
DPDP-XA = DC9X + DPDP-5A   X = 6,7
DPDP-XB = DC10X + DPDP-5B   X = 6,7

LOSP

DC = DCA + DCB

Table C.7 (1/2) Events "DPDP-XA" and "DPDP-XB" (for X=2, 3, 4, 5, 8), "BC-3X" (for X=A, B, C, D, E, F), and "DPDP-1A,-1B" Quantifications

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
DC1X, DC2X, DC3X, DC4X		SINGLE HARDWARE FAULTS TO PANEL DPDP-XA			1.3 E-6			1
DC6, DC8	FUSE	OPENS	1.0 E-6	1	1.0 E-6	3^+, 3^-		2
DC9X, DC10X	SWITCH	CONTACTS N.C. FAILS OPEN	3.0 E-8	1	3.0 E-8	10^+, 10^-		2
	WIRING	SHORT TO GROUND	3.0 E-7	1	3.0 E-7	10^+, 10^-		2
					Σ=1.3 E-6			
DC5, DC7		INSUFFICIENT POWER FROM BATTERY 3A (3B)			6.0 E-6	3^+, 3^-		
	BATTERY	INSUFFICIENT POWER	3.0 E-6	2	6.0 E-6	3^+, 3^-		3
MCC3A-1		MCC BUS 3A UNAVAILABLE			5.6 E-5			5
MCC3B-1		MCC BUS 3B UNAVAILABLE			5.6 E-5			5

Table C.7 (2/2) Events "DCA" and "DCB" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR⁻1)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
DCA		INSUFFICIENT POWER ALL BUSES DC TRAIN A			3.2 E-3			
	BATTERY	INSUFFICIENT POWER	3.0 E-6	1080	3.2 E-3	3^+, 3^-		4
DCB		INSUFFICIENT POWER ALL BUSES DC TRAIN B			3.2 E-3			
	BATTERY	INSUFFICIENT POWER	3.0 E-6	1080	3.2 E-3	3^+, 3^-		4

Table C.7 DC Power

QUANTIFICATION TABLES

NOTES

1 The structure of the fault tree for events DPDP-2A, 3A, 4A, 5A, 8A and DPDP-2B, 3B, 4B, 5B, 8B and BC-3A, 3B, 3C, 3D, 3E, and 3F are all similar.

Each of these events are comprised of the same three single hardware faults and failure of the main DC bus in the train.

2 The DC-system is essentially a monitored system since failures would be detected when they occur. Technical Specifications limit bus outages to two hours. Event unavailability was estimated as the product of event failure frequency and assumed average fault repair time of one hour.

3 The event unavailability was estimated as above (in Note 2), except that the average repair time was assumed to be two hours.

4 For the case of loss of offsite power the unavailability of the batteries dominates the unavailability of each DC-train. The batteries are checked quarterly and it was assumed that battery faults could be discovered at this time. The average fault duration time was thus 1/2 of 3 months.

5 See AC-Power Quantification Tables.

Table C.8 DC Power System - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
DC1X[1]	1.3 E-6
DC2X[1]	1.3 E-6
DC3X[1]	1.3 E-6
DC4X[1]	1.3 E-6
DC6	1.3 E-6
DC8	1.3 E-6
DC9X[1]	1.3 E-6
DC10X[1]	1.3 E-6
DC5	6.0 E-6
DC7	6.0 E-6
MCC3A-1	5.6 E-5
MCC3B-1	5.6 E-5
DCA	3.2 E-3
DCB	3.2 E-3

[1] X=2, 3, 4, 5, 8

APPENDIX D

CLASS I.E. AC POWER SYSTEM

APPENDIX D CLASS I.E. AC POWER SYSTEM

D.1 SYSTEM DESCRIPTION AND OPERATION

The purpose of the class IE electrical system is to provide electric power to those systems required to shut down the reactor and limit the release of radioactive material following a transient or design basis event. AC power is required to operate valves and provide motive power for pumps and fans for all safety systems. The turbine-driven pump in the Emergency Feedwater System is the only safety system pump that does not require AC power. AC power is required during both the injection and recirculation phases of accident sequences. AC power is also supplied to the battery chargers for the 250/125 VDC Battery and Distribution System.

D.1.1 SYSTEM DESCRIPTION

Figure D.1 presents a simplified one line diagram for AC power distribution (the DC power distribution system is also displayed). The preferred power supply for the two redundant 4.16kV Engineered Safeguards (ES) Buses 3A and 3B is the connection to the 230kV substation by means of the Unit 3 startup transformer. The 230kV substation is connected to the existing FPC transmission network by five circuits. The 4.16kV ES buses can also be fed from the Unit 1 and 2 startup transformer provided one of the two units is operating. Similarly, Unit 3 auxiliary transformer can also be used as a source provided the Unit 3 turbine generator is in operation.

Upon loss of electric power due to a separation of the 230kV system, shutdown of the nuclear generating unit electric power will be supplied from the standby power supply which consists of two independent diesel generators. Each diesel generator feeds one of the 4.16kV ES buses. Various ES motor loads are connected to the 4.16kV ES buses by spring breakers. The safeguards auxiliary transformer connections are provided to step-down the 4.16kV for the 480VAC engineered safeguards switchgear centers 3A and 3B. Motor control centers 3A-1, 3A-2, 3A-B, 3B-1 and 3B-2 are provided to feed associated safeguards equipment. MCC 3A-B is switchable between 480V ES Bus 3A or 3B. MCC 3A-1 and 3B-2 supply power to the DC battery chargers as well as power to the inverters in order to provide four independent 120VAC vital buses.

D.1.2 SYSTEM OPERATION

The normal supply for the 4.16kV ES buses 3A and 3B is from the Unit 1 & 2 230kV substation via the Unit 3 startup transformer and "normally closed" feeder breakers 3205 and 3206. The backup connection to Units 1 and 2 startup transformer can be accomplished by manually closing breakers 3211 and 3212.

In the event of the loss of the Unit 3 startup transformer or power at the 230kV substation (resulting in a loss of power on the buses) the following automatic actions occur: breakers 3205 and 3206 open and all breakers on the buses trip with the exception of a pre-selected block (block 1 of Table D.1) of feeder breakers and the 4160/480V ES auxiliary transformer feeder breaker, both diesels start and energize their associated safeguards buses when "normally open" breakers 3209 and 3210 close. Additional equipment is manually reconnected as required for safe plant operation. If there is a requirement for safeguards system operation coincident with the loss of voltage on a 4160V bus, the bus is cleared as before and the diesels are started to energize the bus. However, the remaining selected safeguard loads (Table D.2) are automatically connected within 30 seconds by an orderly sequencing of load timers. In the event the motor driven emergency feedwater pump is required, various decay heat associated loads are disconnected (Table D.2) prior to starting the motor driven emergency feedwater pump to avoid overloading the diesel generator.

Breaker auxiliary contacts and protective relaying are used to supervise contact closures in other safeguards circuits to initiate signals and control opening and closing circuits for breakers in order to prevent bus ties and inadvertent "live" bus transfers.

The 480V engineered safeguards distribution system is contained in two separate 480V unit switch gear rooms 3A and 3B. From these buses, motor control centers 3A-1, 3A-2, 3A-B, 3B-1 and 3B-2 are provided to feed associated safeguards equipment. Although MCC 3A-B is switchable between 480V ES Bus 3A or 3B through a manual transfer switch, it is normally configured to Bus

3A. MCC 3A-1 (and MCC 3B-2) supply redundant DC battery chargers for 250/125VDC Battery and distribution system. MCC 3A-1 also supplies two dual input inverters which in turn supply two 120VAC vital buses 3A and 3C. On loss of AC power the inverter is supplied by the 125VDC batteries to prevent a loss of power on the vital buses. If an inverter is inoperable, a redundant backup path to (MCC 3A-1 supplied) regulated 120VAC is available by manually switching transfer switch VBXS.

Allowable outages for the AC power system are defined by the following general comments on limiting conditions for operation of the class IE AC Electrical Power System. (For a complete description refer to Section 3/4.8.1 of the Technical Specifications.)

- Minimum conditions for operation require:

- 2 operable circuits between offsite transmission network and the onsite class IE Distribution System.

- 2 Diesel Generators (DG's) with associated fuel supplies.

Although various combinations of the above can be inoperable for short durations, the most significant combination allows both DG's to be inoperable for up to two hours provided two offsite AC circuits are shown to be operable. If one DG is not restored within the 2 hour time period, the reactor must be brought to Hot Standby within 6 hours and in Cold Shutdown within the following 30 hours. If only one diesel is inoperable, it must be restored within 72 hours or the reactor must be in Hot Standby within the next 6 hours and in Cold Shutdown within the following 30 hours.

- In addition to the above, all of the Class IE Vital and Safeguards buses must be operable and energized from their normal sources of power. An inoperable bus must be restored to operable status within 8 hours or be in Hot Standby within the next 6 hours and in Cold Shutdown within the following 30 hours.

- Minimum conditions for shutdown require the following buses to be operable and energized from sources of power other than a DG but aligned to an operable DG:

- 1 - 4160V Emergency Bus.
- 1 - 480V Emergency Bus.
- 2 - 120V AC Vital Buses.

Containment integrity must be established within 8 hours if less than the above combination of AC are operable.

Test and surveillance requirements are defined as:

- Each independent circuit between the offsite transmission network and the onsite Class IE Distribution System shall be:
    - Determined operable at least once per 7 days by verifying correct breaker alignments, and sump pumps in tunnel containing DC control feeds to 230kV switchgear are operable.
    - Demonstrated operable at least once per 18 months during shutdown by transferring unit power supply from the normal circuit to the alternate circuit.
- Each diesel generator shall be demonstrated operable at least once per 31 days by verifying fuel level and the diesel is started, synchronized, loaded, and operated for more than 60 minutes. This test can be run during normal operations.
- At least once per 18 months during shutdown:
    - Perform preventive maintenance in accordance with manufacturer's recommendations.
    - Simulate LOSP and ESAS signal to verify automatic load shedding, bus tie breakers open, diesel starts and energizes the auto-connected emergency loads through the load sequencer.
- Emergency AC buses determined operable and energized from normal AC sources at least once per 7 days by verifying correct breaker alignment and indicated power availability.

Table D.1 Block Loading Sequence

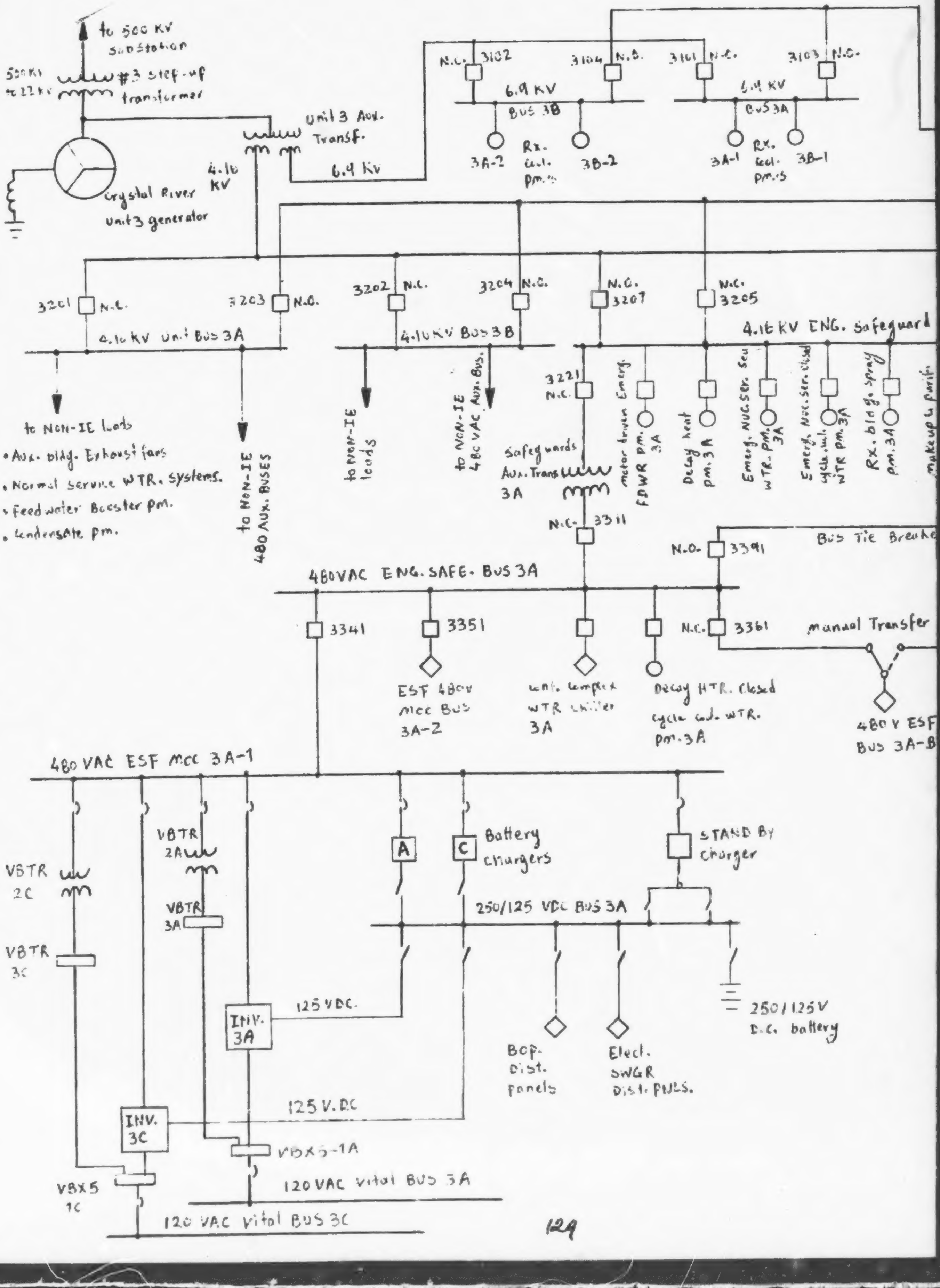
Loading Sequence	Quantity	Description
Block 1	1	Makeup and Purification Pump (High Pressure Inj.)
	1	Decay Heat Pump (Low Pressure Inj.)
		Miscellaneous Valves, Emergency Lighting
	2	Inverters
	1/2	Control Complex Lighting
	2	Battery Chargers
Block 2	2	Reactor Building Fan Assemblies
	1	Emergency Nuclear Services Sea Water Pump
Block 3	1	Emergency Nuclear Services Closed Cycle Cooling Pump
Block 4	1	Decay Heat Service Sea Water Pump
	1	Reactor Building Spray Pump
	1	Decay Heat Closed Cycle Cooling Water Pump

Table D.2 Disconnect Loads and Additional Loads Required

LOADS DISCONNECTED

Decay heat pump
Reactor building spray pump
Decay heat service sea water pump
Decay heat closed cycle cooling water pump

BEST DOCUMENT AVAILABLE


to 500 KV substation
500 KV to 22 KV
#3 step-up transformer
Crystal River Unit 3 generator
Unit 3 Aux. Transf.
4.16 KV
6.9 KV
N.C. 3102
3104 N.O.
3101 N.C.
3103 N.O.
6.9 KV BUS 3B
6.9 KV BUS 3A
3A-2
Rx. cool. pm.'s
3B-2
3A-1
Rx. cool. pm.'s
3B-1
3201 N.C.
3203 N.O.
3202 N.C.
3204 N.O.
N.C. 3207
N.C. 3205
4.16 KV Unit Bus 3A
4.16 KV Bus 3B
4.16 KV ENG. Safeguard
to NON-IE loads
• Aux. bldg. Exhaust fans
• Normal service WTR. systems.
• Feedwater Booster pm.
• Condensate pm.
to NON-IE 480 AUX. BUSES
to NON-IE loads
to NON-IE 480 VAC Aux. Bus.
3221 N.C.
Safeguards Aux. Trans 3A
motor driven Emerg. FDWR pm. 3A
Decay heat pm. 3A
Emerg. NUC. Ser. Sea WTR. pm. 3A
Emerg. Nuc. Ser. Closed cycle cool. WTR pm. 3A
Rx. bldg. spray pm. 3A
makeup & purif.
N.C. 3311
N.O. 3391
Bus Tie Breake
480 VAC ENG. SAFE. BUS 3A
3341
3351
N.C. 3361
Manual Transfer
ESF 480V MCC Bus 3A-2
Cont. Complex WTR Chiller 3A
Decay HTR. Closed cycle cool. WTR. pm. 3A
480 V ESF Bus 3A-B
480 VAC ESF MCC 3A-1
VBTR 2C
VBTR 3C
VBTR 2A
VBTR 3A
A
C
Battery chargers
STAND BY charger
250/125 VDC BUS 3A
125 VDC.
INV. 3A
INV. 3C
125 V.DC
250/125 V D.C. battery
BOP. Dist. panels
Elect. SWGR Dist. PNLS.
VBXS-1A
VBXS 1C
120 VAC Vital BUS 3A
120 VAC Vital BUS 3C

BEST DOCUMENT AVAILABLE

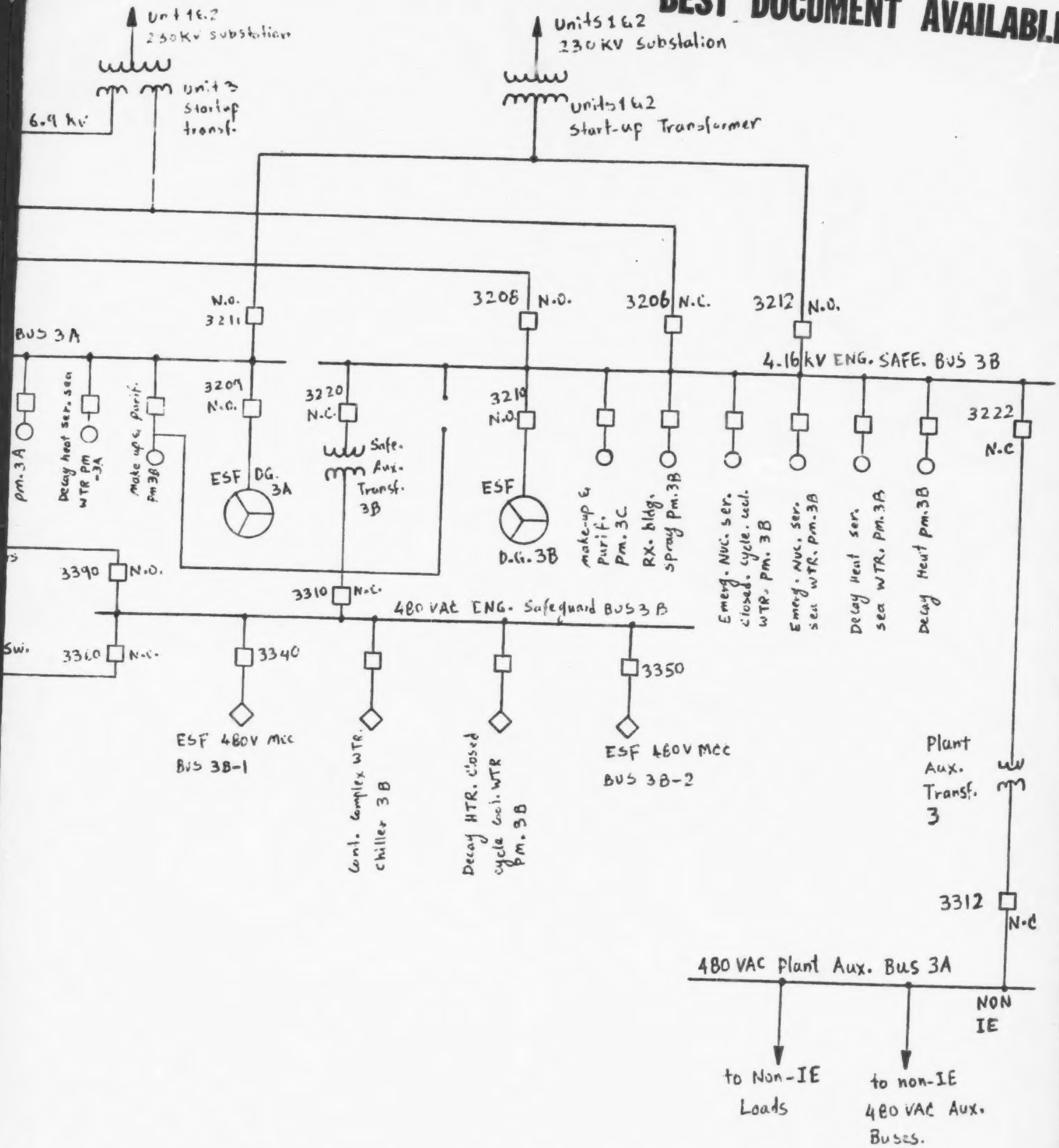

Unit 1&2
230KV substation
unit 3
Startup
transf.
6.9 kv
Units 1&2
230 KV Substation
Units 1&2
Start-up Transformer
N.O.
3211
3208 N.O.
3206 N.C.
3212 N.O.
BUS 3A
4.16 kV ENG. SAFE. BUS 3B
3209
N.C.
3220
N.C.
3210
N.O.
3222
N.C
pm. 3A
Decay heat ser. sea WTR Pm -3A
make up & Purif. Pm 3B
ESF DG. 3A
Safe. Aux. Transf. 3B
ESF
D.G. 3B
make-up & Purif. Pm. 3C
RX. bldg. spray Pm. 3B
Emerg. Nuc. ser. closed. cycle. ccl. WTR. Pm. 3B
Emerg. Nuc. ser. sea WTR. Pm. 3B
Decay Heat ser. sea WTR. Pm. 3A
Decay Heat Pm. 3B
3390 N.O.
Sw.
3360 N.C.
3310 N.C.
480 VAC ENG. Safeguard BUS 3B
3340
3350
ESF 480V MCC
BUS 3B-1
Cntl. Complex WTR. chiller 3B
Decay HTR. closed cycle ccl. WTR Pm. 3B
ESF 480V MCC
BUS 3B-2
Plant
Aux.
Transf.
3
3312
N.C
480 VAC Plant Aux. Bus 3A
NON
IE
to Non-IE
Loads
to non-IE
480 VAC Aux.
Busses.

Figure D.1 Class IE AC Power System - Simplified One-Line Diagram

D.2 SYSTEM SIMPLIFIED FAULT TREES

Fault Trees were drawn for each of three levels of emergency power distribution: 4160V, 480V and 120VAC. The simplified fault trees are shown in Figure D.2. The fault summary is shown in Table D.3.

4160V FAULT TREE

Two fault trees were developed: one for loss of offsite power (LOSP) as the initiating event, and the other for accident initiators other than LOSP. The difference being, of course, that in the latter case offsite power must fail in addition to the diesels. No credible single failures could be postulated which would fail both DG buses. Dominant cut sets for loss of both buses involve failure of the diesels to start, or to continue to run. Some of the faults associated with loss of power on the 4.16kV buses are due to failures with protective relaying and logic such that automatic starting, load sequencing and circuit breaker trips are not accomplished. Common mode events include diesel common mode and hardware double failures such as the bus tie circuit breakers not opening.

One major assumption for this tree is that turbine trip occurs on LOSP which leaves only Units 1 and 2 and the DG's available to provide emergency power. Technical Specifications require as a minimum two 4.16kV buses, two 480VAC buses (3A&3B), and four 120VAC vital buses available unless the plant is in cold shutdown or refueling.

480VAC FAULT TREES

Individual simplified trees were constructed for each of the seven MCC ES 480V buses. In keeping with the simplified tree requirements, general cable and bus open and short to power or ground were not considered on the basis of probability of occurrence. Thus, for the most part, each individual 480V MCC tree is represented by faults associated with its feeder breaker or loss of power supplied to the bus. Transfers are provided for other ES systems whose components require power from one or more of these buses. Bus operability is also discussed in Section D.1.2 of this report.

120VAC VITAL BUSES

Similarly as was done for the 480VAC buses, each of the four 120VAC vital buses were modeled individually to facilitate transfers. Single failures for these buses are associated with faults which cause a disruption of power to the vital bus, e.g., fuse and breaker faults, switch failures, etc. Double failures (due to symmetry each of the trees are exactly alike) are associated with loss of power from the inverter system and loss of power from the backup 120VAC redundant regulated power supplies. This backup source is provided essentially only for maintenance purposes on the inverter and requires switching the manual transfer switch VBXS by the operator. This human interface is reflected on the tree. The inverter system failures are represented by single faults with the inverter itself or doubles reflecting the loss of the normal inverter 480VAC input and the "uninterruptible" backup connection to the DC power system.

Table D.3 (1/4) AC Power Fault Summary - 4.16kV Buses 3A, 3B

SIMPLIFIED FAULT TREE - FAULT SUMMARY

EVENT NAME	EVENT COMPONENT	FAILURE MODE
K000001W	Loss of Offsite Power	Conditional Event
KDL0013R	Diesel Generator A	Does Not Run
KDL0013S	Diesel Generator A	Does Not Start
KLC0013W	Relay Logic for Automatic Start	Fails to Function
KLC003AW	Bus 3A Load Shedding Logic	Fails to Function
KCB0010P	Circuit Breaker 3206	Does Not Open
KLC0010W	Relay Logic for CB 3206	Fails to Function
KCB0011P	Circuit Breaker 3205	Does Not Open
KLC0011W	Relay Logic for CB 3205	Fails to Function
KCB0012N	Circuit Breaker 3209	Does Not Close
KCB0012W	Relay Logic for CB 3209	Fails to Function
E0000DC1	DC Control Power "A"	DC Power Not Available
KDL0023R	Diesel Generator B	Does Not Run
KDL0023S	Diesel Generator B	Does Not Start
KLC0023W	Relay Logic for Automatic Start	Fails to Function
KLC003BW	Bus 3B Load Shedding Logic	Fails to Function
KCB0024N	Circuit Breaker 3210	Does Not Close
KLC0024W	Relay Logic for CB 3210	Fails to Function
KCB0025P	Circuit Breaker 3222	Does Not Open
KLC0025W	Relay Logic for CB 3222	Fails to Function
T000ESA1	Engineering Safeguards Signal	No Actuation Signal
E0000DC2	DC Control Power "B"	DC Power Not Available
K0000DLW	Diesel Generators 3A, 3B	Common Mode
K House 01	Electrical Train "B" Out for Service	Not a Fault Event
K House 02	Electrical Train "A" Out for Service	Not a Fault Event
E0000DCW	Loss of all DC Power	Conditional Event

Table D.3 (2/4) AC Power Fault Summary - 480V MCC Buses

SIMPLIFIED FAULT TREE - FAULT SUMMARY		
EVENT NAME	EVENT COMPONENT	FAILURE MODE
KCB0006X	Circuit Breaker 3341	Operator Error (Commission)
KLC0006W	Relay Logic for CB 3341	Premature Transfer
KCB0007X	Circuit Breaker 3311	Operator Error (Commission)
KLC0007W	Relay Logic for CB 3311	Premature Transfer
KCB0008X	Circuit Breaker 3221	Operator Error (Commission)
KLC0008W	Relay Logic for CB 3221	Premature Transfer
KCB0014X	Circuit Breaker 3351	Operator Error (Commission)
KLC0014W	Relay Logic for CB 3351	Premature Transfer
KCB0015X	Circuit Breaker 3361	Operator Error (Commission)
KLC0015W	Relay Logic for CB 3361	Premature Transfer
KSW0016X	MCC 3A-B Transfer Switch	Operator Error (Omission)
KSW0016N	MCC 3A-B Transfer Switch	Does Not Close
KCB0017X	Circuit Breaker 3360	Operator Error (Commission)
KLC0017W	Relay Logic for CB 3360	Premature Transfer
KCB0018X	Circuit Breaker 3340	Operator Error (Commission)
KLC0018W	Relay Logic for CB 3340	Premature Transfer
KCB0019X	Circuit Breaker 3310	Operator Error (Commission)
KLC0019W	Relay Logic for CB 3310	Premature Transfer
KCB0020X	Circuit Breaker 3220	Operator Error (Commission)
KLC0020W	Relay Logic for CB 3200	Premature Transfer
KCB0021X	Circuit Breaker 3350	Operator Error (Commission)
KLC0021W	Relay Logic for CB 3350	Premature Transfer
KTR0030D	Safeguards Auxiliary Transformer 3A	Shorts
KTR0031D	Safeguards Auxiliary Transformer 3B	Shorts

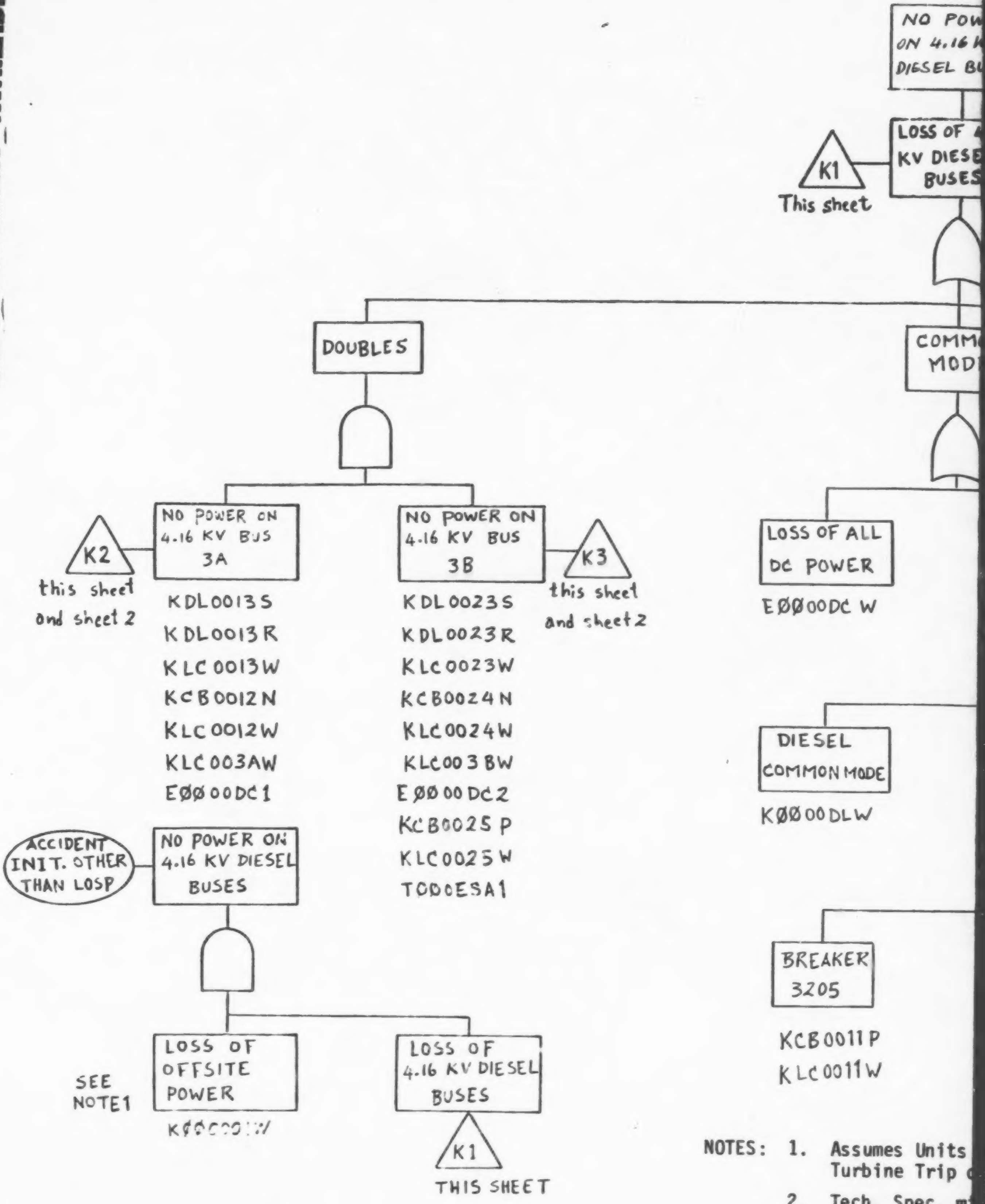
Table D.3 (3/4) AC Power Fault Summary - 120VAC Vital Bus 3A and 3C

SIMPLIFIED FAULT TREE - FAULT SUMMARY		
EVENT NAME	EVENT COMPONENT	FAILURE MODE
KCB00A1X	Circuit Breaker 3601	Operator Error (Commission)
KFU00A6B	Fuse VBF1	Opens
KSW00A2B	Manual XFR Switch 3A VBXS-1A	Opens
KSW00A2X	Manual XFR Switch 3A VBXS-1A	Operator Error (Omission)
KSW00A2N	Manual XFR Switch 3A VBXS-1A	Does Not Close
KIV00A5W	Invertor 3A	Fails to Function
KFU00A7B	Fuse VBF45	Opens
KCB00A8X	Breaker to Inverter 3A	Operator Error (Commission)
KLC00A8W	Relay Logic for Inverter 3A CB	Fails to Function
KFU00A9B	Fuse VBF 36	Opens
KVR0A10W	VBTR-3A 15W Power Supply/Regulator 3A	Fails to Function
KFU0A11B	Fuse VBF35	Opens
KTR0A12D	Voltage Transformer VBTR-2A	Shorts
KCB00A4X	Circuit Breaker to VBTR-2A	Operator Error (Commission)
KLC00A4W	Relay Logic for CB to VBTR-2A	Fails to Function
KCB00C1X	Circuit Breaker 3603	Operator Error (Commission)
KFU00C6B	Fuse VBF 2	Opens
KSW00C2B	Manual XFR Switch VBXS-3C	Opens
KSW00C2X	Manual XFR Switch VBXS-3C	Operator Error (Omission)
KSW00C2N	Manual XFR Switch VBXS-3C	Does Not Close
KIV00C5W	Inverter 3C	Fails to Function
KFU00C7B	Fuse VBF 49	Opens
KCB00C7X	Breaker to Inverter 3C	Operator Error (Commission)
KLC00C8W	Relay Logic for Inverter 3C CB	Fails to Function
KFU00C9B	Fuse VBF 40	Opens
KVR0C10W	VBTR-3C 15W Redundant PS Regulator 3C	Fails to Function
KFU0C11B	Fuse VBF 39	Opens
KTR0C12D	Voltage Transformer VBTR-2C	Shorts
KCB00C4X	Circuit Breaker to VBTR-2C	Operator Error (Commission)
KLC00C4W	Relay Logic for CB to VBTR-2	Fails to Function

Table D.3 (4/4) AC Power Fault Summary - 120VAC Vital Bus 3B and 3D

SIMPLIFIED FAULT TREE - FAULT SUMMARY		
EVENT NAME	EVENT COMPONENT	FAILURE MODE
KCB00B1X	Circuit Breaker 3602	Operator Error (Commission)
KFU00B6B	Fuse VBF 3	Opens
KSW00B2B	Manual XFR Switch VBXS-3B	Opens
KSW00B2X	Manual XFR Switch VBXS-3B	Operator Error (Omission)
KSW00B2N	Manual XFR Switch VBXS-3B	Does Not Close
KIV00B5W	Inverter 3B	Fails to Function
KFU00B7B	Fuse VBF 47	Opens
KCB00B8X	Breaker to Inverter 3B	Operator Error (Commission)
KLC00B8W	Relay Logic for Inverter 3B CB	Fails to Function
KFU00B9B	Fuse VBF 38	Opens
KVR0B10W	VBTR 3B 15W Redundant PS Regulator 3B	Fails to Function
KFU0B11B	Fuse VBF 37	Opens
KTR0B12D	Voltage Transformer VBTR-2B	Shorts
KCB00B4X	Circuit Breaker to VBTR-2B	Operator Error (Commission)
KLC00B4W	Relay Logic for CB to VBTR-2B	Fails to Function
KCB00D1X	Circuit Breaker 3604	Operator Error (Commission)
KFU00D6B	Fuse VBF 4	Opens
KSW00D2B	Manual XFR Switch VBXS-1D	Opens
KSW00D2X	Manual XFR Switch VBXS-1D	Operator Error (Omission)
KSW00D2N	Manual SFR Switch VBSX-1D	Does Not Close
KIV00D5W	Inverter 3D	Fails to Function
KFU00D7X	Fuse VBF 51	Opens
KCB00D8X	Breaker to Inverter 3D	Operator Error (Commission)
KLC00D8W	Relay Logic for Inverter 3D CB	Fails to Function
KFU00D9B	Fuse VBF 42	Opens
KVR0D10W	VBTR-3D 15W Redundant PS Regulator 3D	Fails to Function
KFU0D11B	Fuse VBF 41	Opens
KTR0D12D	Voltage Transformer VBTR-2D	Shorts
KCB00D4X	Circuit Breaker to VBTR-2D	Operator Error (Commission)
KLC00D4W	Relay Logic for CB to VBTR-2D	Fails to Function

BEST DOCUMENT AVAILABLE


NO POW
ON 4.16 K
DIESEL BU
LOSS OF
KV DIESE
BUSES
K1
This sheet
DOUBLES
COMM
MOD
NO POWER ON 4.16 KV BUS 3A
K2
this sheet and sheet 2
KDL0013S
KDL0013R
KLC0013W
KCB0012N
KLC0012W
KLC003AW
E0000DC1
NO POWER ON 4.16 KV BUS 3B
K3
this sheet and sheet 2
KDL0023S
KDL0023R
KLC0023W
KCB0024N
KLC0024W
KLC003BW
E0000DC2
KCB0025P
KLC0025W
TODOESA1
LOSS OF ALL DC POWER
E0000DC W
DIESEL COMMON MODE
K0000DLW
ACCIDENT INIT. OTHER THAN LOSP
NO POWER ON 4.16 KV DIESEL BUSES
BREAKER 3205
KCB0011P
KLC0011W
SEE NOTE1
LOSS OF OFFSITE POWER
K000001W
LOSS OF 4.16 KV DIESEL BUSES
K1
THIS SHEET

NOTES: 1. Assumes Units
Turbine Trip

2. Tech. Spec. m
shutdown: one
bus (3A or 3B)

BEST DOCUMENT AVAILABLE

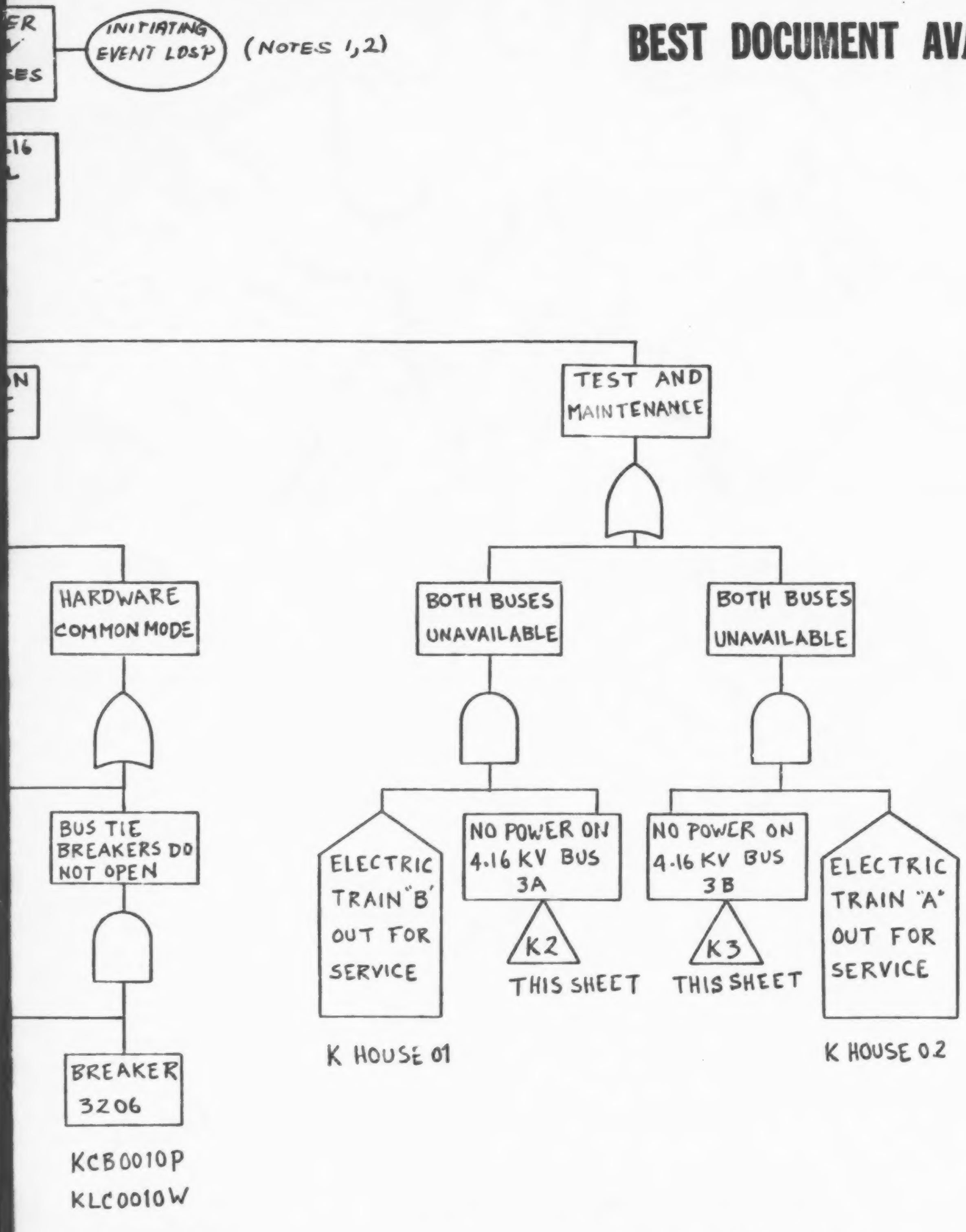

ER
V
ES
INITIATING EVENT LOSP
(NOTES 1,2)
.16
L
N
TEST AND MAINTENANCE
HARDWARE COMMON MODE
BOTH BUSES UNAVAILABLE
BOTH BUSES UNAVAILABLE
BUS TIE BREAKERS DO NOT OPEN
ELECTRIC TRAIN "B" OUT FOR SERVICE
NO POWER ON 4.16 KV BUS 3A
K2
THIS SHEET
NO POWER ON 4.16 KV BUS 3B
K3
THIS SHEET
ELECTRIC TRAIN "A" OUT FOR SERVICE
K HOUSE 01
K HOUSE 02
BREAKER 3206
KCB0010P
KLC0010W

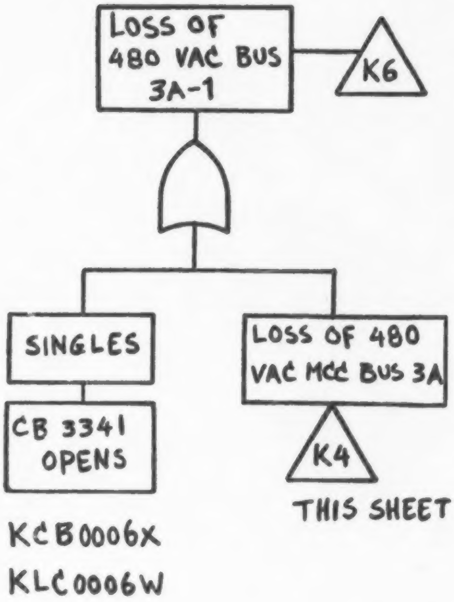
Figure D.2 (1/4) Simplified Fault Tree -
AC Power System (4160VAC Buses)

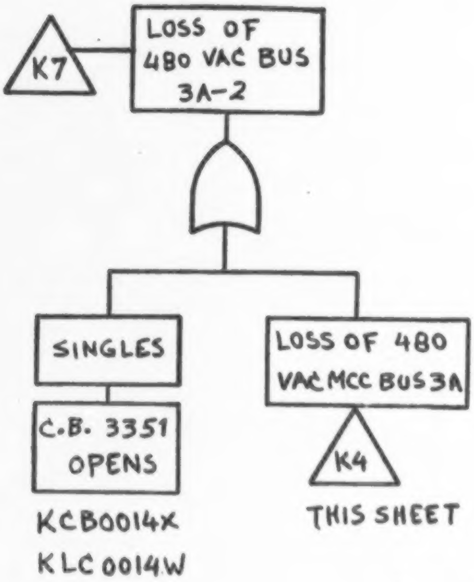
1 & 2 are down and
ccurs on LOSP

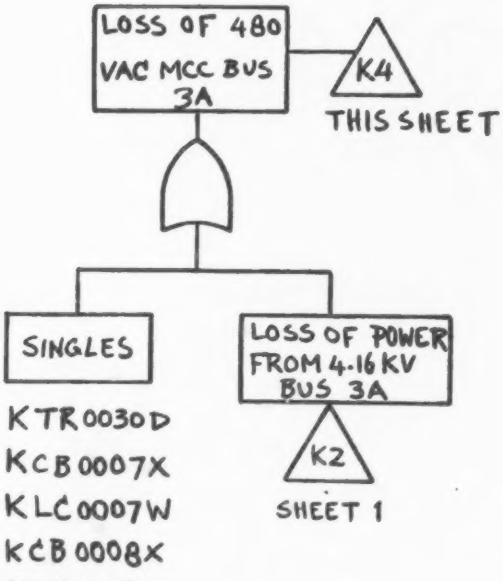
imum required for
.1kV bus; one 480VAC
two 120VAC vital buses.

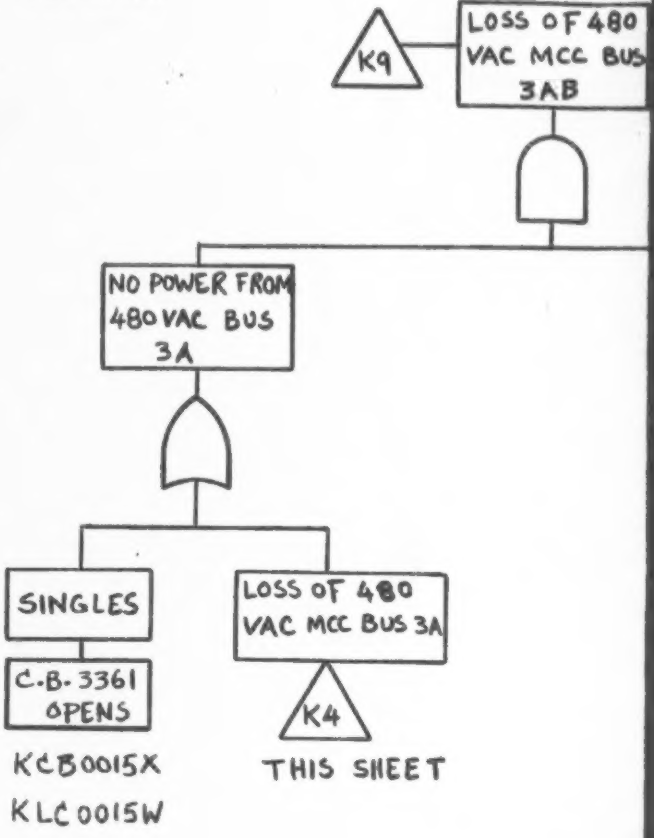
[redacted]

BEST DOCUMENT AVAILABLE


LOSS OF 480 VAC BUS 3A-1
K6
SINGLES
CB 3341 OPENS
KCB0006X
KLC0006W
LOSS OF 480 VAC MCC BUS 3A
K4
THIS SHEET


K7
LOSS OF 480 VAC BUS 3A-2
SINGLES
C.B. 3351 OPENS
KCB0014X
KLC0014W
LOSS OF 480 VAC MCC BUS 3A
K4
THIS SHEET


LOSS OF 480 VAC MCC BUS 3A
K4
THIS SHEET
SINGLES
KTR0030D
KCB0007X
KLC0007W
KCB0008X
KLC0008W
LOSS OF POWER FROM 4.16 KV BUS 3A
K2
SHEET 1


K9
LOSS OF 480 VAC MCC BUS 3AB
NO POWER FROM 480 VAC BUS 3A
SINGLES
C.B. 3361 OPENS
KCB0015X
KLC0015W
LOSS OF 480 VAC MCC BUS 3A
K4
THIS SHEET

BEST DOCUMENT AVAILABLE

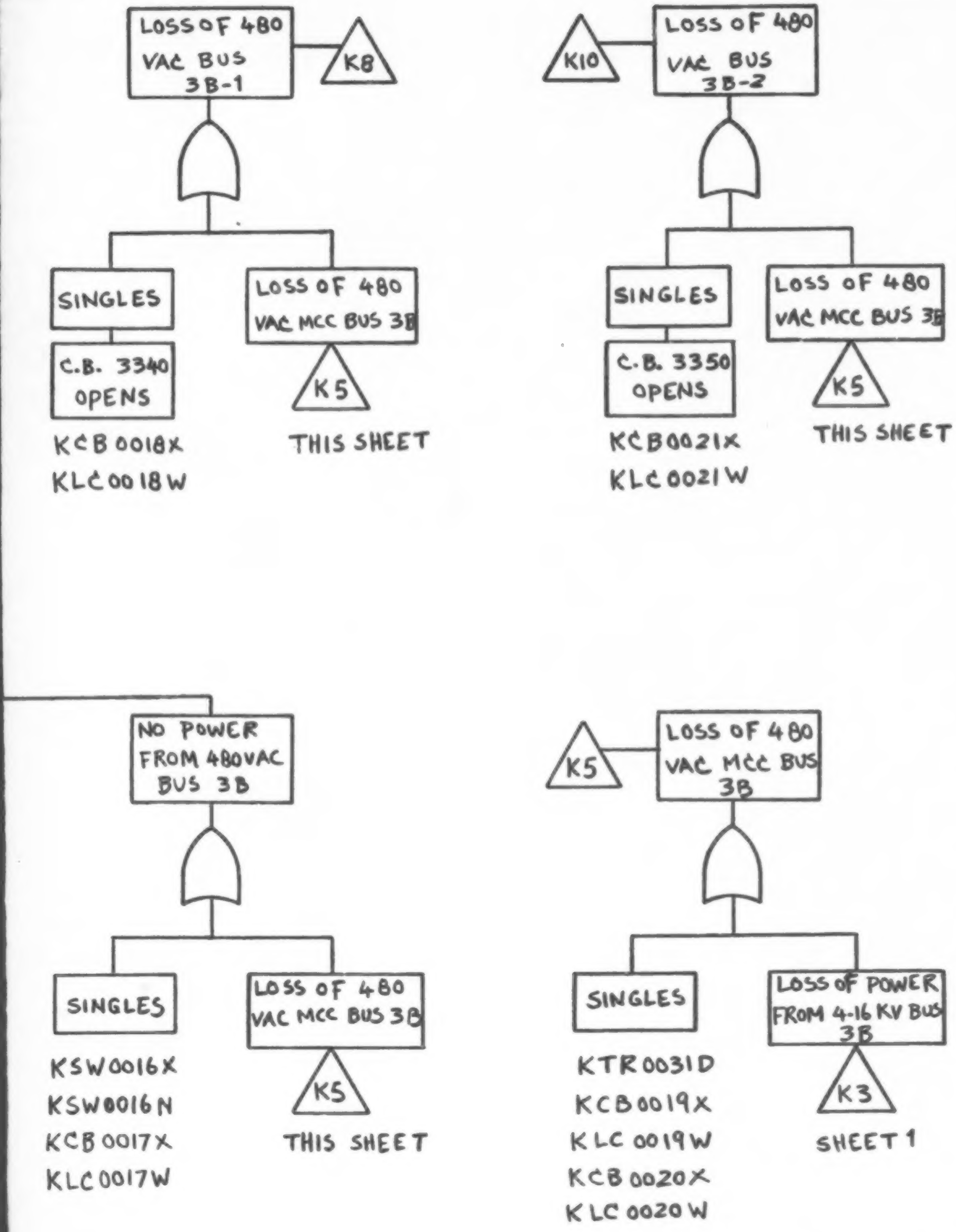
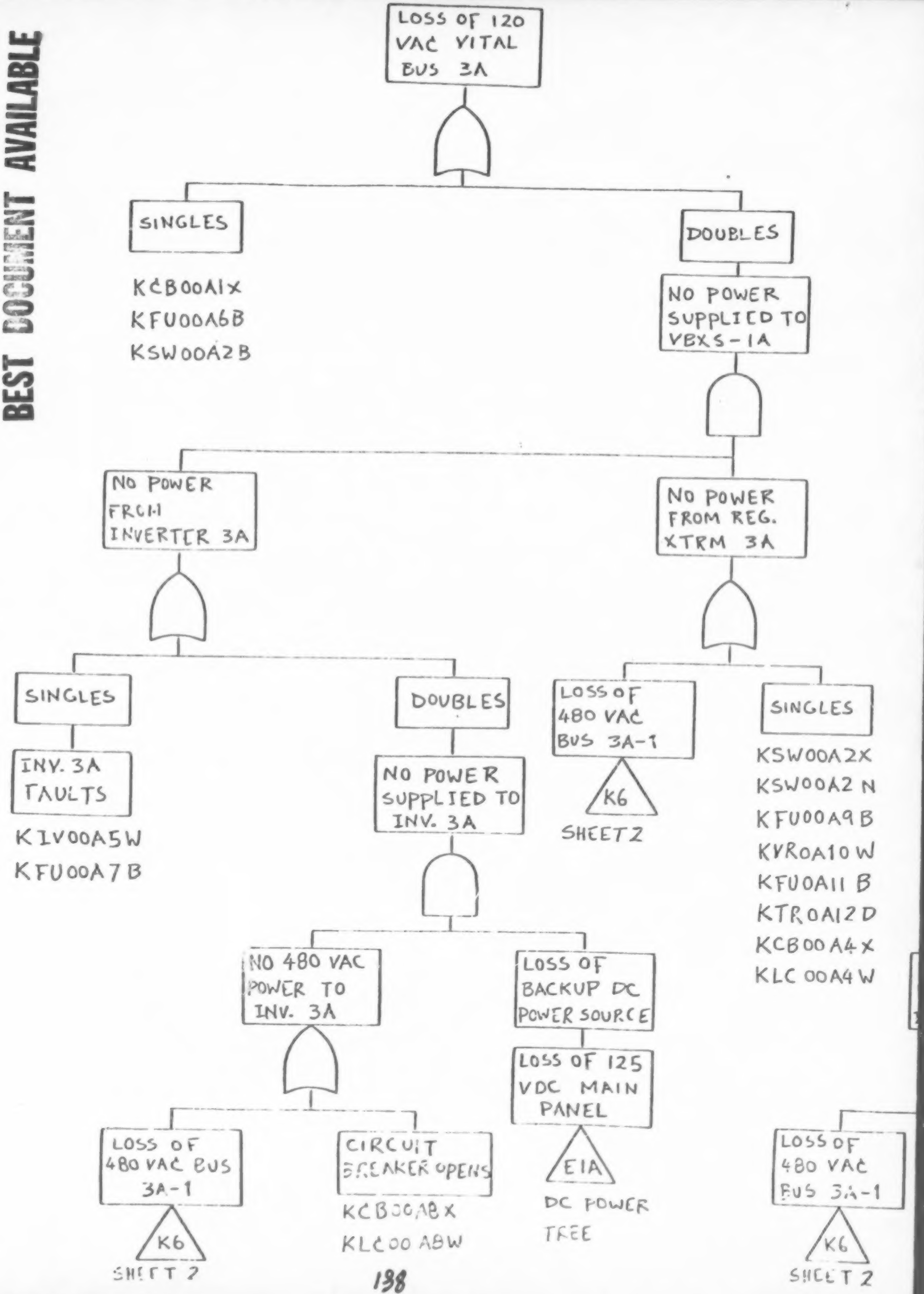

LOSS OF 480 VAC BUS 3B-1
K8
SINGLES
C.B. 3340 OPENS
KCB 0018X
KLC 0018W
LOSS OF 480 VAC MCC BUS 3B
K5
THIS SHEET
K10
LOSS OF 480 VAC BUS 3B-2
SINGLES
C.B. 3350 OPENS
KCB 0021X
KLC 0021W
LOSS OF 480 VAC MCC BUS 3B
K5
THIS SHEET
NO POWER FROM 480VAC BUS 3B
SINGLES
KSW0016X
KSW0016N
KCB 0017X
KLC 0017W
LOSS OF 480 VAC MCC BUS 3B
K5
THIS SHEET
K5
LOSS OF 480 VAC MCC BUS 3B
SINGLES
KTR 0031D
KCB 0019X
KLC 0019W
KCB 0020X
KLC 0020W
LOSS OF POWER FROM 4-16 KV BUS 3B
K3
SHEET 1

Figure D.2 (2/4) Simplified Fault Tree - AC Power System (Individual 480VAC MCCs)

BEST DOCUMENT AVAILABLE


LOSS OF 120 VAC VITAL BUS 3A
SINGLES
KCB00A1X
KFU00A6B
KSW00A2B
DOUBLES
NO POWER SUPPLIED TO VBXS-1A
NO POWER FROM INVERTER 3A
NO POWER FROM REG. XTRM 3A
SINGLES
INV. 3A FAULTS
KIV00A5W
KFU00A7B
DOUBLES
NO POWER SUPPLIED TO INV. 3A
LOSS OF 480 VAC BUS 3A-1
K6
SHEET 2
SINGLES
KSW00A2X
KSW00A2N
KFU00A9B
KVR0A10W
KFU0A11B
KTR0A12D
KCB00A4X
KLC00A4W
NO 480 VAC POWER TO INV. 3A
LOSS OF BACKUP DC POWER SOURCE
LOSS OF 125 VDC MAIN PANEL
E1A
DC POWER TREE
LOSS OF 480 VAC BUS 3A-1
K6
SHEET 2
CIRCUIT BREAKER OPENS
KCB00A8X
KLC00A8W
LOSS OF 480 VAC BUS 3A-1
K6
SHEET 2

BEST DOCUMENT AVAILABLE

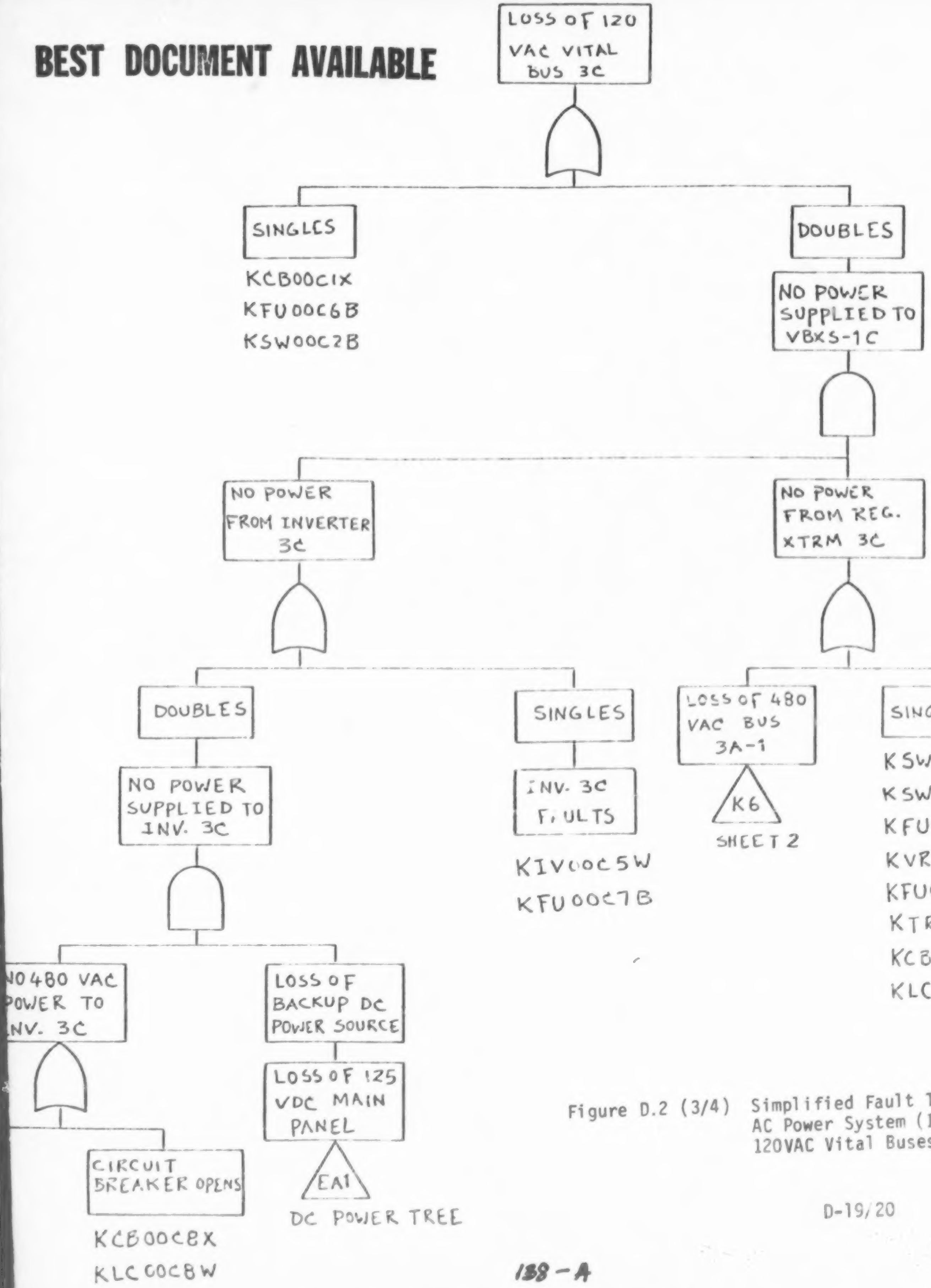
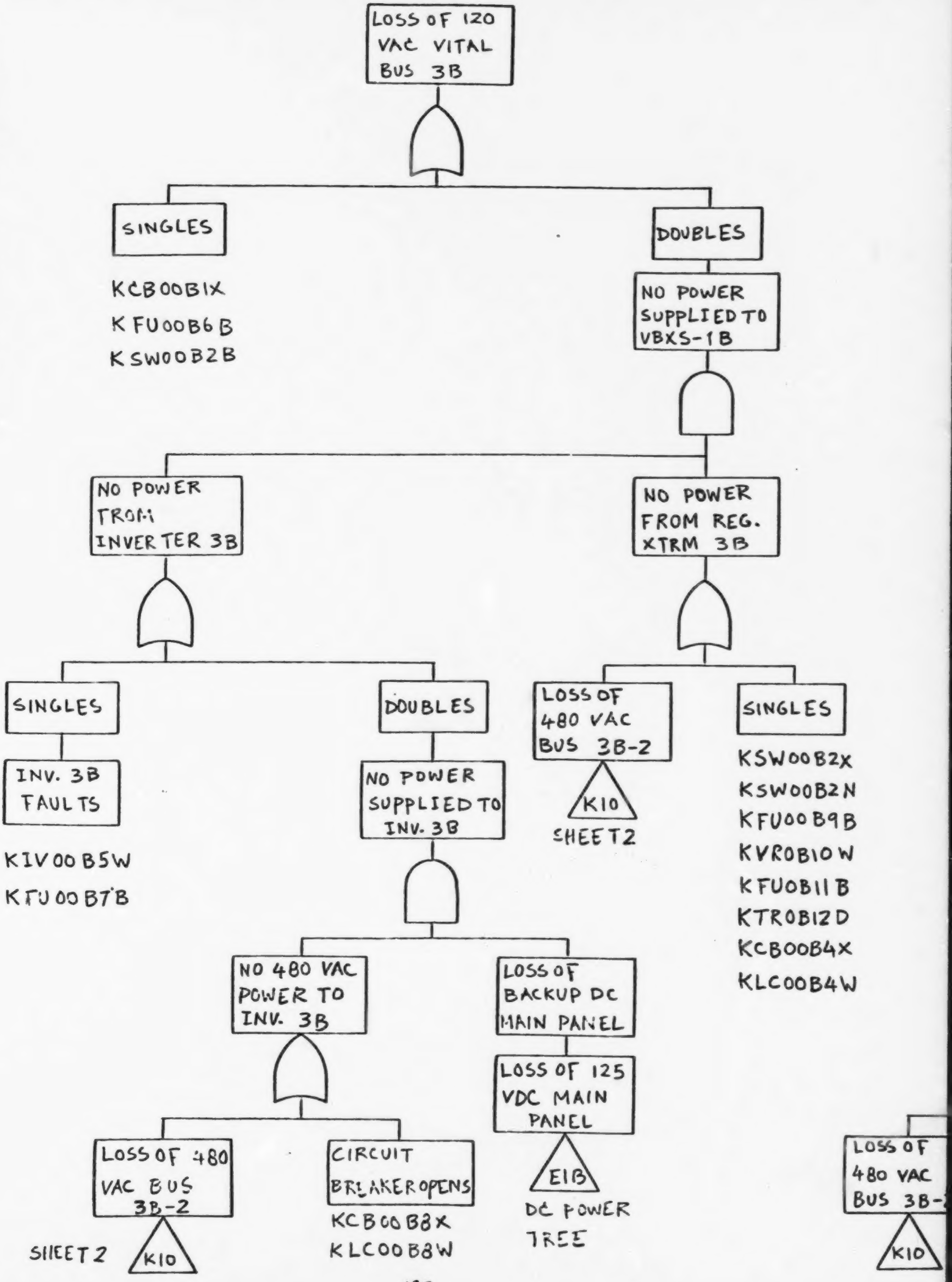

LOSS OF 120 VAC VITAL BUS 3C
SINGLES
KCB00C1X
KFU00C6B
KSW00C2B
DOUBLES
NO POWER SUPPLIED TO VBXS-1C
NO POWER FROM INVERTER 3C
NO POWER FROM REG. XTRM 3C
DOUBLES
SINGLES
LOSS OF 480 VAC BUS 3A-1
K6
SHEET 2
SINGLES
KSW00C2X
KSW00C2N
KFU00C7B
KVR0C10W
KFU0C11B
KTR0C12D
KCB00C4X
KLC00C4W
NO POWER SUPPLIED TO INV. 3C
INV. 3C FAULTS
KIV00C5W
KFU00C7B
NO 480 VAC POWER TO INV. 3C
LOSS OF BACKUP DC POWER SOURCE
LOSS OF 125 VDC MAIN PANEL
EA1
DC POWER TREE
CIRCUIT BREAKER OPENS
KCB00C8X
KLC00C8W

Figure D.2 (3/4) Simplified Fault Tree - AC Power System (Individual 120VAC Vital Buses A, C)

BEST DOCUMENT AVAILABLE


LOSS OF 120 VAC VITAL BUS 3B
SINGLES
KCB00B1X
KFU00B6B
KSW00B2B
DOUBLES
NO POWER SUPPLIED TO VBXS-1B
NO POWER FROM INVERTER 3B
NO POWER FROM REG. XTRM 3B
SINGLES
INV. 3B FAULTS
KIV00B5W
KFU00B7B
DOUBLES
NO POWER SUPPLIED TO INV. 3B
LOSS OF 480 VAC BUS 3B-2
K10
SHEET 2
SINGLES
KSW00B2X
KSW00B2N
KFU00B9B
KVR0B10W
KFU0B11B
KTR0B12D
KCB00B4X
KLC00B4W
NO 480 VAC POWER TO INV. 3B
LOSS OF BACKUP DC MAIN PANEL
LOSS OF 125 VDC MAIN PANEL
E1B
DC POWER TREE
LOSS OF 480 VAC BUS 3B-2
SHEET 2
K10
CIRCUIT BREAKER OPENS
KCB00B8X
KLC00B8W
LOSS OF 480 VAC BUS 3B-
K10

BEST DOCUMENT AVAILABLE

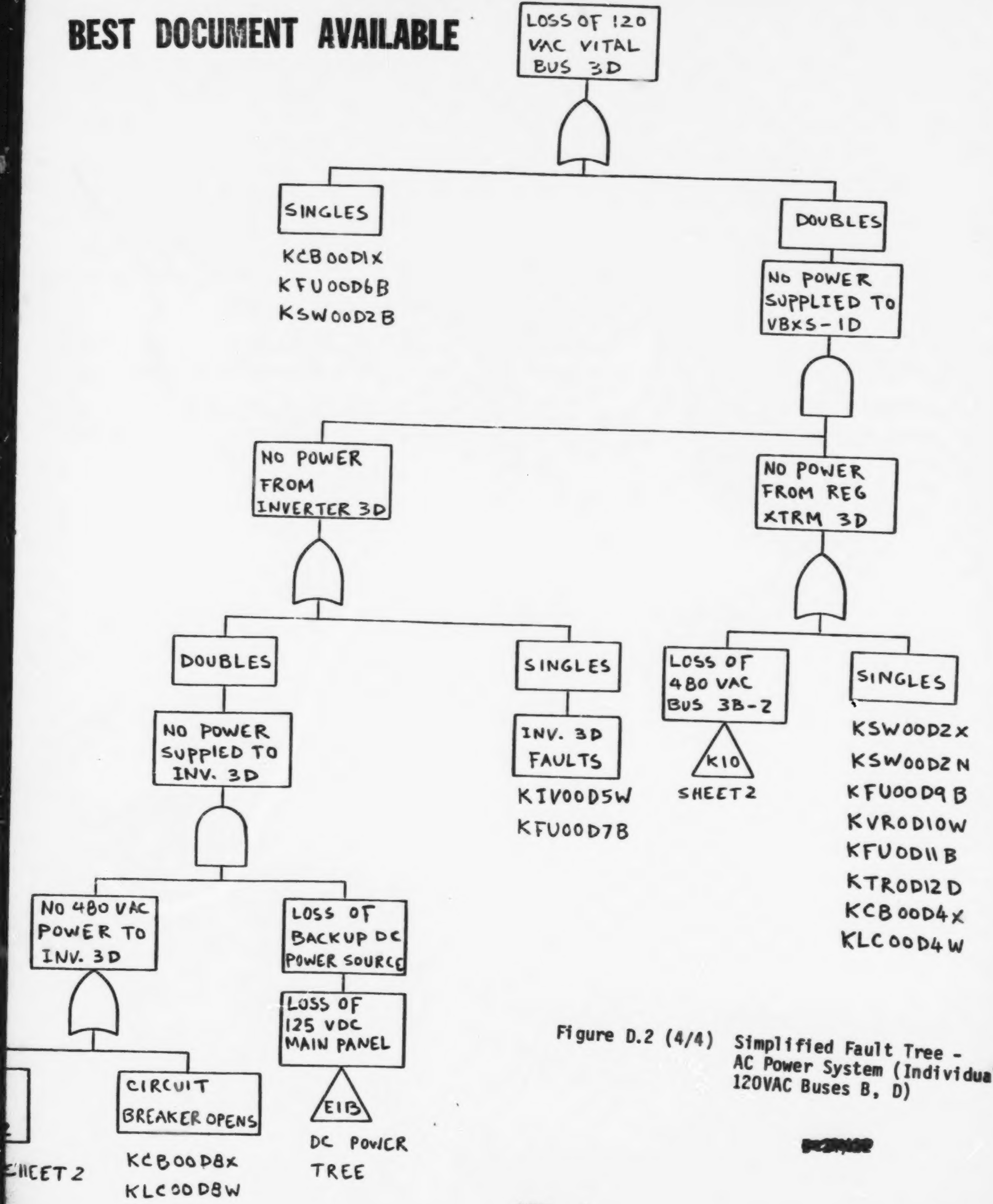

LOSS OF 120 VAC VITAL BUS 3D
SINGLES
KCB00D1X
KFU00D6B
KSW00D2B
DOUBLES
NO POWER SUPPLIED TO VBXS-1D
NO POWER FROM INVERTER 3D
NO POWER FROM REG XTRM 3D
DOUBLES
SINGLES
LOSS OF 480 VAC BUS 3B-2
K10
SHEET 2
SINGLES
KSW00D2X
KSW00D2N
KFU00D9B
KVR0D10W
KFU0D11B
KTR0D12D
KCB00D4X
KLC00D4W
NO POWER SUPPIED TO INV. 3D
INV. 3D FAULTS
KIV00D5W
KFU00D7B
NO 480 VAC POWER TO INV. 3D
LOSS OF BACKUP DC POWER SOURCE
LOSS OF 125 VDC MAIN PANEL
E1B
DC POWER TREE
CIRCUIT BREAKER OPENS
KCB00D8X
KLC00D8W
HEET 2

Figure D.2 (4/4) Simplified Fault Tree - AC Power System (Individual 120VAC Buses B, D)

D.3 SYSTEM QUANTIFICATION

D.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The Crystal River AC power distribution system is a two train system with the capability of being energized by multiple sources. The preferred source, and the one that the distribution system is normally aligned with, is the 230kV substation through the Unit 3 startup transformer. However, if power from the 230kV substation is not available, the distribution system may be aligned to receive power from either Units 1 or 2 (if they are available) or from the onsite diesel generators. This realignment requires the availability of DC power. AC power is supplied to the various safety systems from a variety of buses on both (independent) trains.

For the case where offsite power is available, the unavailability of the major AC buses was assessed to be primarily due to premature transfer of breakers and transformer shorts during a time window that would make the bus unavailable, but would not require the plant to be shut down (by Technical Specification limits). Since these faults are relatively rare in occurrence, and since the fault exposure time is small, the unavailability of individual buses was assessed to be small compared to other faults. The unavailability of an entire train of AC power is smaller still.

For the loss of offsite power case the unavailability of the AC power trains was assessed to be a contributor to safety system unavailability. The major contributors to AC power unavailability (both single trains and both trains) were assessed to be due to failures and maintenance outages of the diesel generators coupled with the unavailability of power from Units 1 and 2. Failure of a battery in the DC power distribution system was a less important contributor.

D.3.2 SYSTEM FAULT TREE QUANTIFICATION

This section presents the quantification of the AC power fault tree for emergency operation in response to an accident or transient. Only AC power availability during the injection phase of an accident or transient is presented. AC power failure during the recirculation phase was assessed to be of negligible probability compared to other safety system failures for the following reasons:

- For the case where offsite power is available, failure of individual AC buses by premature breaker transfers could probably be recovered within an acceptable time frame to mitigate the accident. These failures are of small probability compared to other safety system failure modes, at any rate. Loss of an entire train of AC power is an even smaller probability event.
- For the case where loss of offsite power is the initiating event, it was assumed that offsite power would be restored by the time that the recirculation phase started. This assumption was based on WASH 1400 data that show that the probability of restoration of offsite power three to ten hours after offsite power is lost is very high. Other options for recovering power by the recirculation phase include restoration of diesels that may have failed at the onset of the accident (Units 1 and 2 require offsite power for restart).

Modularized fault trees were constructed for each of the 4160VAC and 480VAC buses with offsite power available. For the loss of offsite power case, modularized fault trees were constructed for AC power Trains A and B, and for total loss of AC power.

Table D.4 shows the success requirements for AC power distribution, Table D.5 contains the top event definition for the modularized fault trees, and Figures D.3 through D.9 show the modularized fault trees for both the LOSP and Non-LOSP cases. The unavailability of each gate is shown on these trees, as well as the unavailability of the top events. Table D.6 presents the Boolean equations that represent the fault trees. Table D.7, the quantification table, shows the quantification of each gate, by component and failure mode. The attached notes describe the assumptions used in the quantification. Table D.8 summarizes the point estimates and the error factors for each gate.

Table D.4 AC Power

SUCCESS REQUIREMENTS

INITIATOR	TRAINS	NOTES
B1, B2, B3, B4 All Transients	1/1 480V, 4160V buses	1,2
LOSP	1/2 AC power trains	1,2,3

NOTES:

1. Train A of AC power supplies power to the A trains of engineered safety systems. Train B supplies power to the B trains of these systems.

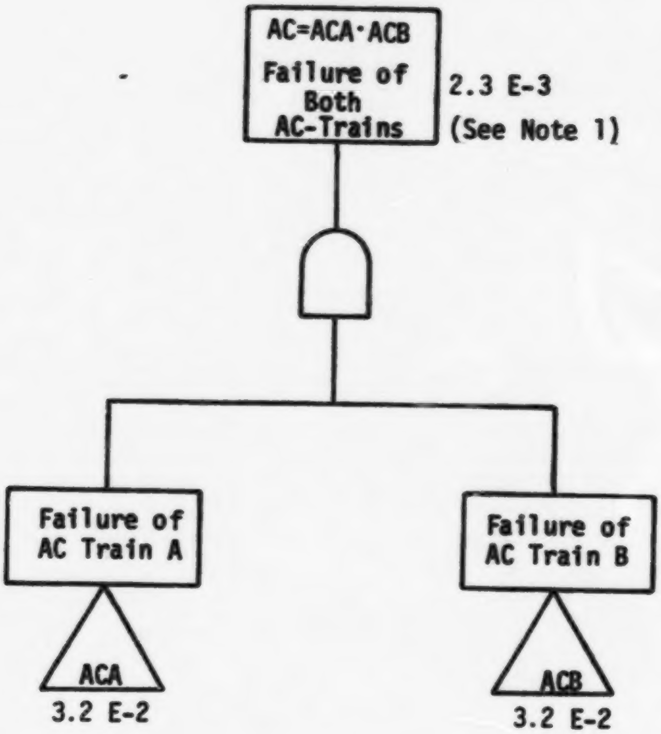
2. Analysis was performed for individual 480V buses for the case where offsite power is available. Analysis was performed for the A and B trains of AC power for the loss of offsite power case. No analysis was performed for the 120V AC vital buses for the offsite power available case, since these involve failures of the 480V buses, coupled with additional failures, which make the failure probabilities negligible.

3. For the loss of offsite power case, credit is given for obtaining power from units 1 and 2 through the auxiliary transformer. An assessment of the availability of this additional backup power source is contained in the analysis.

Table D.5 AC Power

TOP EVENT DEFINITIONS

BOOLEAN REPRESENTATION	TOP EVENT	NOTES
Non-LOSP-CASE		
3A1	No power on 480VAC bus 3A-1	
MCC3A	No power on 480VAC bus MCC3A	
3A2	No power on 480VAC bus 3A-2	
3B1	No power on 480VAC bus 3B-1	
MCC3B	No power on 480VAC bus MCC-3B	
3B2	No power on 480VAC bus 3B-2	
MCC3AB	No power on 480VAC bus 3AB	
LOSP-CASE		
ACA	No power on 4160V ESF bus 3A	
ACB	No power on 4160V ESF bus 3B	
AC	No power on either 4160V ESF bus 3A and 3B	
A2	No power available from Units 1 and 2	


AC=ACA·ACB
Failure of Both AC-Trains
2.3 E-3
(See Note 1)
Failure of AC Train A
Failure of AC Train B
ACA
3.2 E-2
ACB
3.2 E-2

NOTE: (1) ACA and ACB are not independent, thus Boolean reduction is required to evaluate AC.

Figure D.3 Modularized Fault Tree for Event "AC" (LOSP)

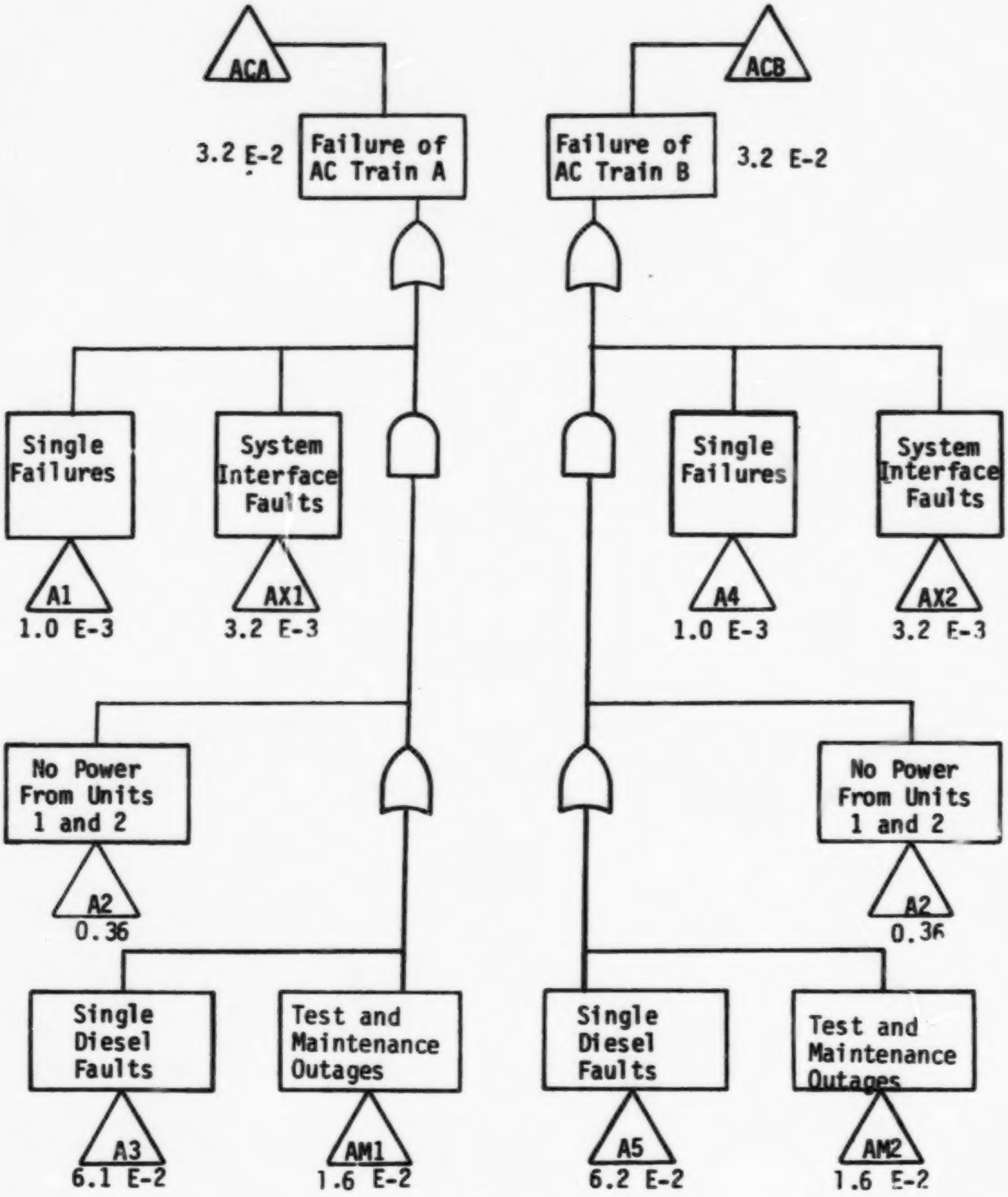

ACA
3.2 E-2
Failure of AC Train A
ACB
Failure of AC Train B
3.2 E-2
Single Failures
A1
1.0 E-3
System Interface Faults
AX1
3.2 E-3
Single Failures
A4
1.0 E-3
System Interface Faults
AX2
3.2 E-3
No Power From Units 1 and 2
A2
0.36
No Power From Units 1 and 2
A2
0.36
Single Diesel Faults
A3
6.1 E-2
Test and Maintenance Outages
AM1
1.6 E-2
Single Diesel Faults
A5
6.2 E-2
Test and Maintenance Outages
AM2
1.6 E-2

Figure D.4 Modularized Fault Trees for Events "ACA" and "ACB" (LOSP)

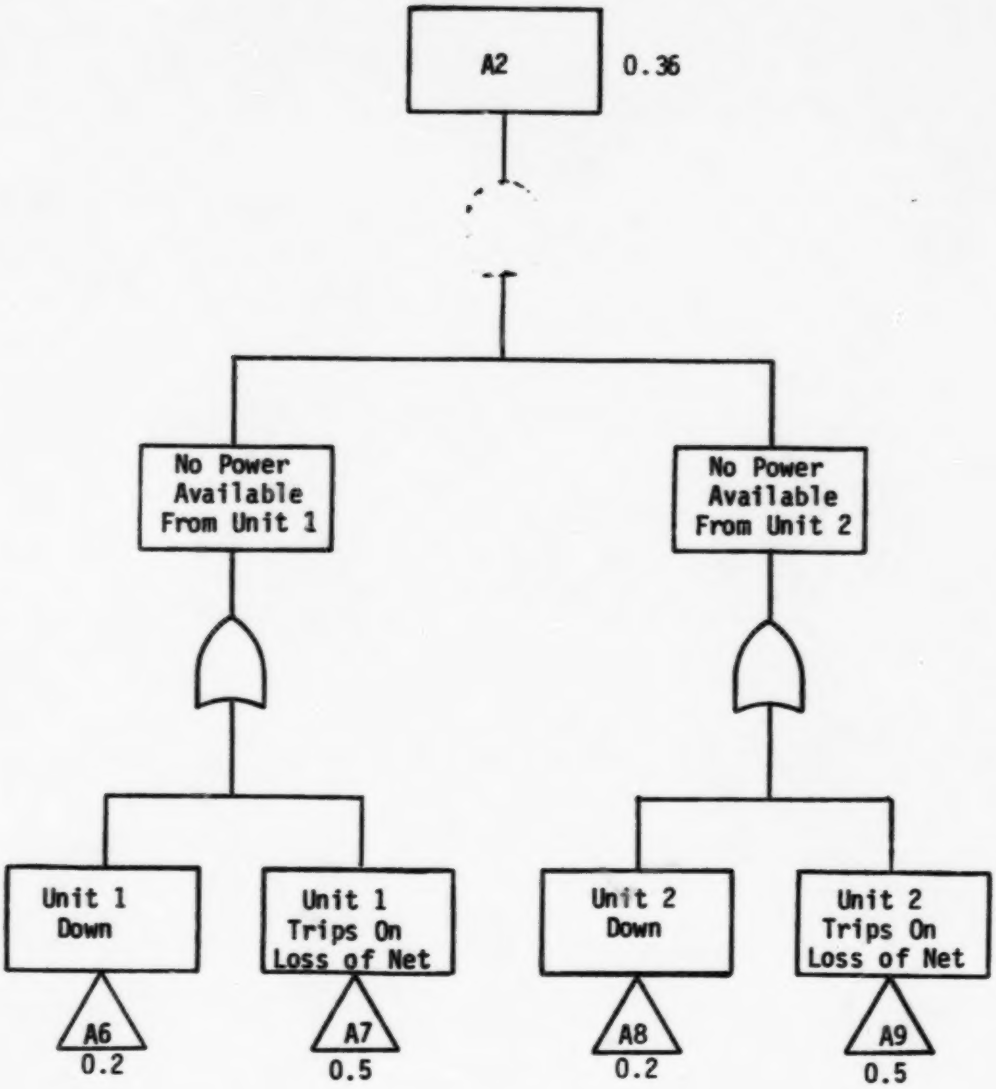

A2
0.36
No Power Available From Unit 1
No Power Available From Unit 2
Unit 1 Down
Unit 1 Trips On Loss of Net
Unit 2 Down
Unit 2 Trips On Loss of Net
A6
0.2
A7
0.5
A8
0.2
A9
0.5

Figure D.5 Modularized Fault Tree for Event "A2" (LOSP)

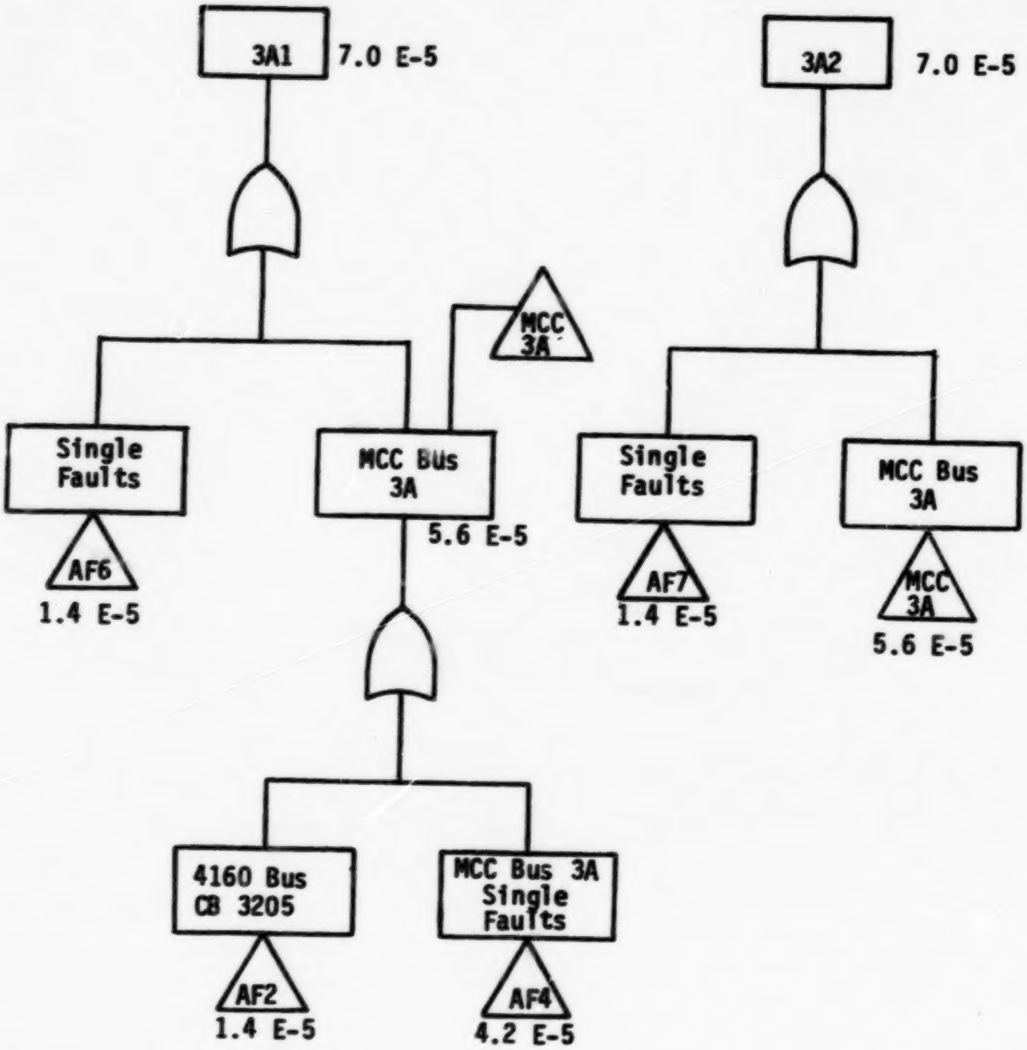

3A1
7.0 E-5
3A2
7.0 E-5
MCC 3A
Single Faults
MCC Bus 3A
5.6 E-5
Single Faults
MCC Bus 3A
AF6
1.4 E-5
AF7
1.4 E-5
MCC 3A
5.6 E-5
4160 Bus CB 3205
MCC Bus 3A Single Faults
AF2
1.4 E-5
AF4
4.2 E-5

Figure D.6 Modularized Fault Trees for Events "3A-1" and "3A-2" (Non-LOSP)

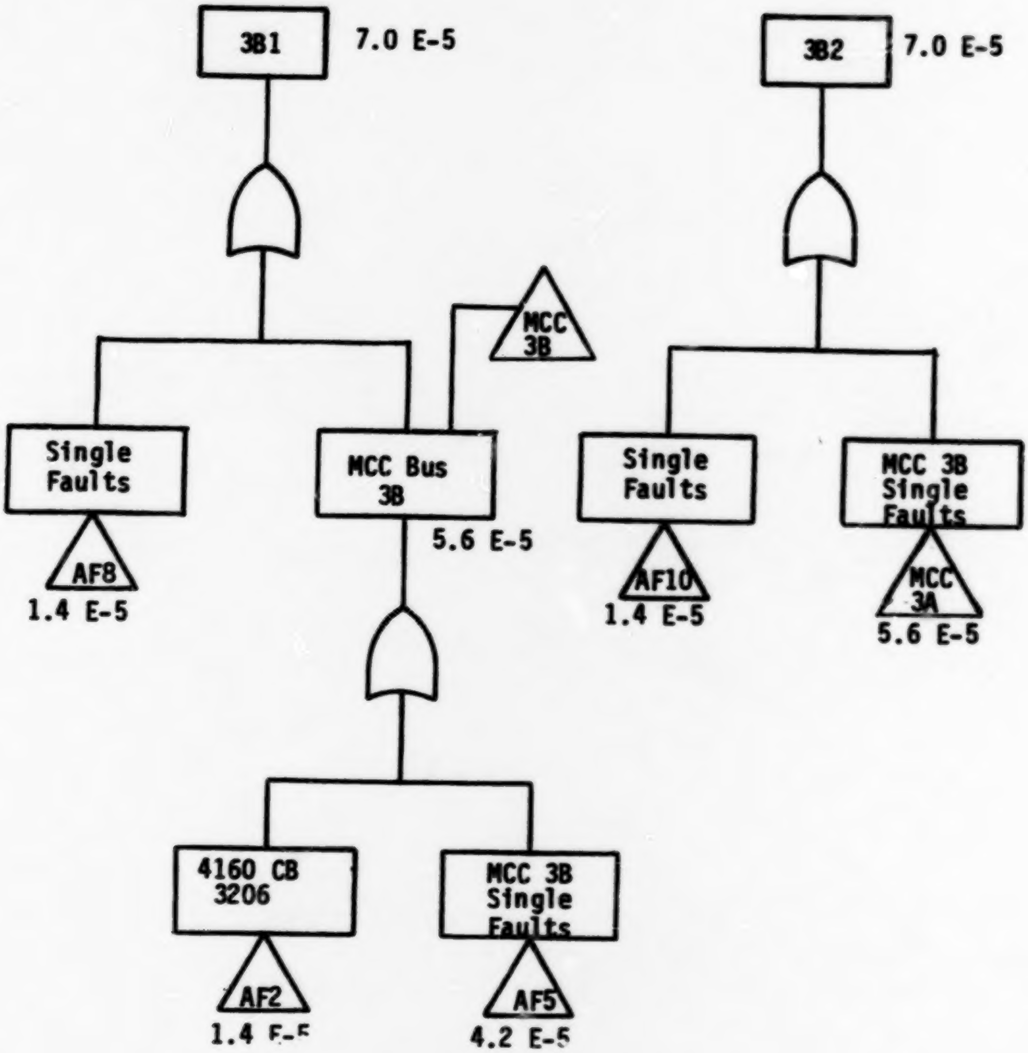

3B1
7.0 E-5
MCC 3B
Single Faults
AF8
1.4 E-5
MCC Bus 3B
5.6 E-5
4160 CB 3206
AF2
1.4 E-5
MCC 3B Single Faults
AF5
4.2 E-5
3B2
7.0 E-5
Single Faults
AF10
1.4 E-5
MCC 3B Single Faults
MCC 3A
5.6 E-5

Figure D.7 Modularized Fault Trees for Events "3B-1" and "3B-2" (Non-LOSP)

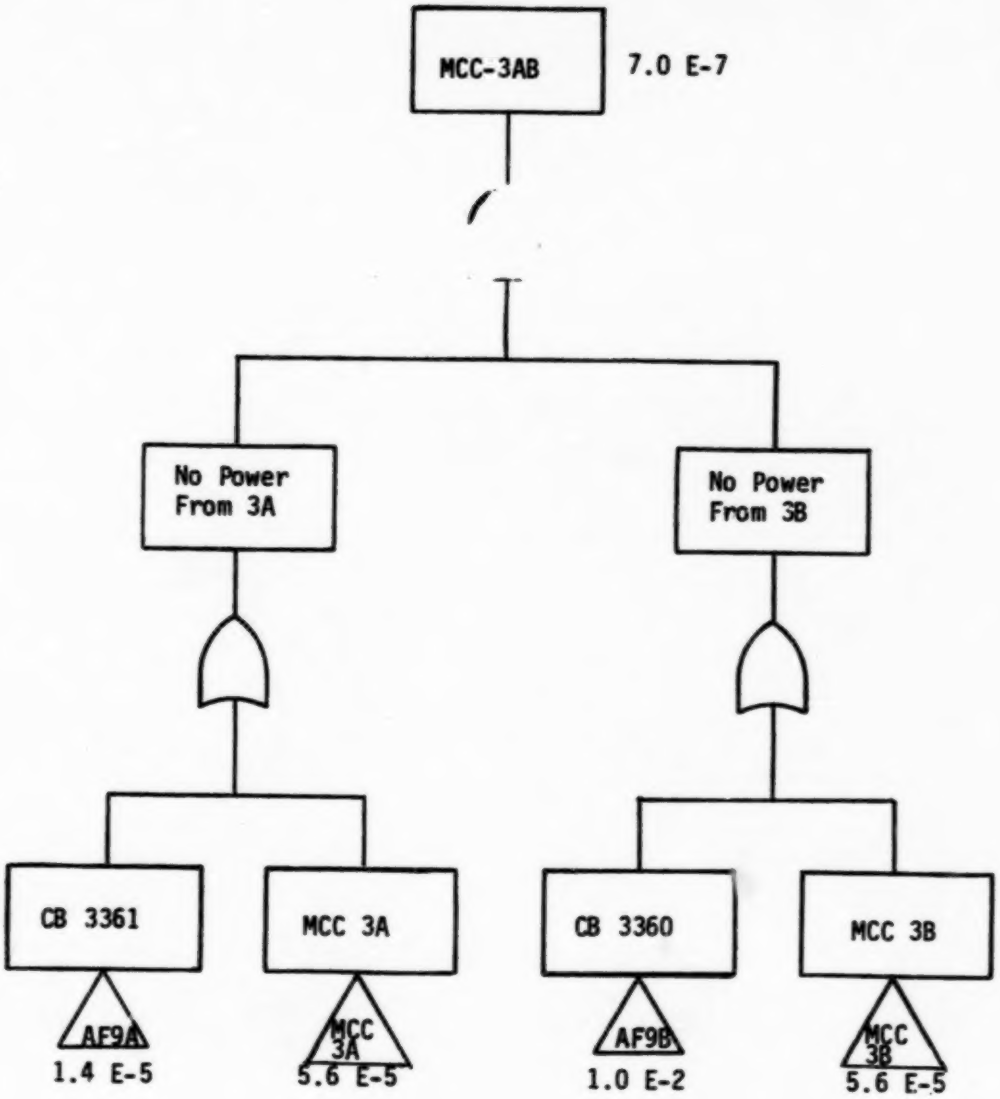

MCC-3AB
7.0 E-7
No Power From 3A
No Power From 3B
CB 3361
MCC 3A
CB 3360
MCC 3B
AF9A
1.4 E-5
MCC 3A
5.6 E-5
AF9B
1.0 E-2
MCC 3B
5.6 E-5

Figure D.8 Modularized Fault Tree for Event "MCC-3AB" (Non-LOSP)

Table D.6 (1/2) AC - Power LOSP

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS — **NOTES**

$\mathrm{AC = ACA \cdot ACB}$ (1)

INTERMEDIATE EVENTS

$\mathrm{ACA = A1 + AX1 + A2 \cdot (A3 + AM1)}$

$\mathrm{ACB = A4 + AX2 + A2 \cdot (A5 + AM2)}$

$\mathrm{A2 = (A6 + A7) \cdot (A8 + A9)}$

$\mathrm{AX1 = DCA}$

$\mathrm{AX2 = DCB}$

BOOLEAN EQUATIONS REGROUPED FOR BOOLEAN REDUCTION

TOP EVENT

$$\mathrm{AC = (A1 + AX1) \cdot [A4 + AX2 + A2 \cdot (A5 + AM2)] +}$$
$$\mathrm{+ A2 \cdot [(A4 + AX2) \cdot (A3 + AM1) + A3 \cdot A5 + A3 \cdot AM2 + A5 \cdot AM1]}$$ (2)

INTERMEDIATE EVENTS

SAME AS ABOVE

NOTES: 1. This event AC is not Boolean reduced.

2. The event $\mathrm{AM1 \cdot AM2}$ is prohibited by Technical Specifications and is therefore not included.

Table D.6 (2/2) AC - Power Non-LOSP

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS

3A1 = AF6 + MCC3A

3A2 = AF7 + MCC3A

3B1 = AF8 + MCC3B

3B2 = AF10 + MCC3B

3AB = (AF9A + MCC3A)·(AF9B + MCC3B)

INTERMEDIATE EVENTS

MCC3A = AF1 + AF4

MCC3B = AF2 + AF5

BEST DOCUMENT AVAILABLE

Table D.7 (1/5) Events "ACA" and "A2" Quantification (LOSP)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR-1)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
A1		SINGLE FAILURES TO TRAIN A			1.0 E-3			
	CIRCUIT BKR 3205	FAILS TO TRANSFER	D		1.0 E-3	$3^+, 3^-$		
A2		POWER FROM UNITS 1 AND 2 NOT AVAILABLE			0.36			
A6	UNIT 1	DOWN	D		0.2			6
A7	UNIT 1	TRIPS ON LOSS OF NET	D		0.5			7
A8	UNIT 2	DOWN	D		0.2			6
A9	UNIT 2	TRIPS ON LOSS OF NET	D		0.5			7
					$\pi(\Sigma)=$ 0.36			
A3		SINGLE FAULTS THAT FAIL POWER FROM DIESEL 3A			6.1 E-2			
	DG-3A	FAILS TO START	D		3.0 E-2	$3^+, 3^-$		
	DG-3A	FAILS TO RUN	3.0 E-3	10	3.0 E-2	$10^+, 10^-$		1
	RELAY LOGIC	AUTO START FAILS TO FUNCTION			NOT SIGNIFICANT			2
	CIRCUIT BKR 3209	FAILS TO CLOSE	D		1.0 E-3	$3^+, 3^-$		
	RELAY LOGIC	CIRCUIT BREAKER FAILS TO FUNCTION			NOT SIGNIFICANT			2
	LOAD SHED. LOGIC	FAILS TO FUNCTION			NOT SIGNIFICANT			2
					$\Sigma=$6.1 E-2			
AX1		SYSTEM INTERFACE FAULTS			3.2 E-3			
DCA	DC TRAIN A	FAILS ON LOSP			3.2 E-3			8
AM1		TRAIN A TEST & MAINTENANCE OUTAGES			1.6 E-2			3
	DG-3A	OUT FOR TEST	3/720	3	1.3 E-2	$3^+, 3^-$	H	
	DG-3A	OUT FOR UNSCHEDULED MAINTENANCE	2/8760	15	3.5 E-3	$3^+, 3^-$	M	
					$\Sigma=$ 1.6 E-2			

BEST DOCUMENT AVAILABLE

Table D.7 (2/5) Event "ACB" Quantification (LOSP)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
A4		SINGLE FAILURES TO TRAIN B			1.0 E-3			
	CIRCUIT BKR 3206	FAILS TO TRANSFER	D		1.0 E-3	3^+, 3^-		
A2		POWER FROM UNITS 1 AND 2 NOT AVAILABLE (SEE EVENT ACA)			0.36			
A5		SINGLE FAULTS THAT FAIL POWER FROM DIESEL 3B			6.2 E-2			
	DG-3B	FAILS TO START	D		3.0 E-2	3^+, 3^-		
	DG-3B	FAILS TO RUN	3.0 E-3	10	3.0 E-2	10^+, 10^-		1
	RELAY LOGIC	AUTO START FAILS TO FUNCTION			NOT SIGNIFICANT			2
	CIRCUIT BKR 3210	FAILS TO CLOSE	D		1.0 E-3	3^+, 3^-		
	RELAY LOGIC	CIRCUIT BREAKER LOGIC FAILS TO FUNCTION			NOT SIGNIFICANT			2
	LOAD SHED. LOGIC	FAILS TO FUNCTION			NOT SIGNIFICANT			2
	CIRCUIT BKR 3312	FAILS TO OPEN	D		1.0 E-3	3^+, 3^-		2
	RELAY LOGIC	CIRCUIT BREAKER FAILS TO FUNCTION			NOT SIGNIFICANT			2
	ESAS-B	NO ESAS SIGNAL AND NO RECOVERY	D		NOT SIGNIFICANT			2
					Σ=6.2 E-2			
AX2		SYSTEM INTERFACE FAULTS			3.2 E-3			
DCB	DC TRAIN B	FAILS ON LOSP			3.2 E-3			8
AM2		TRAIN B TEST & MAINTENANCE OUTAGES			1.6 E-2			3
	DG-3B	OUT FOR TEST	3/720	3	1.3 E-2	3^+, 3^-	M	
	DG-3B	OUT FOR UNSCHEDULED MAINTENANCE	2/8760	15	3.5 E-3	3^+, 3^-	M	
					Σ= 1.6 E-2			

Table D.7 (3/5) Events "3A-1" and "MCC-3A" Quantification (Non-LOSP)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR-1)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
AF6		SINGLE FAULTS TO EVENT 3A-1			1.4 E-5			
	CIRCUIT BKR 3341	PREMATURE TRANSFER (OPEN)	1.0 E-6	14	1.4 E-5	3^{+}, 3^{-}		4
MCC3A		MCC BUS 3A UNAVAILABLE			5.6 E-5			
AF1		SINGLE FAULTS, 4160V BUS A			1.4 E-5			
	CIRCUIT BKR 3205	PREMATURE TRANSFER	1.0 E-6	14	1.4 E-5	3^{+}, 3^{-}		4
AF4		MCC BUS 3A SINGLE FAULTS			4.2 E-5			
	TRANSFORMER 3A	SAFEGUARD AUX. TRANSFORMER 3A SHORTS	1.0 E-6	4	4.0 E-6	3^{+}, 3^{-}		4
	TRANSFORMER 3A	FAILS TO OPERATE	1.0 E-6	10	1.0 E-5	3^{+}, 3^{-}		5
	CIRCUIT BKR 3311	PREMATURE TRANSFER (OPEN)	1.0 E-6	14	1.4 E-5	3^{+}, 3^{-}		4
	CIRCUIT BKR 3221	PREMATURE TRANSFER (OPEN)	1.0 E-5	14	1.4 E-5	3^{+}, 3^{-}		4
					Σ=4.2 E-5			

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table D.7 (4/5) Events "3A-2", "3B-1", and "3B-2" Quantification (Non-LOSP)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR⁻1)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
AF7		SINGLE FAULTS TO EVENT 3A-2			1.4 E-5			
	CIRCUIT BKR 3351	PREMATURE TRANSFER (OPEN)	1.0 E-6	14	1.4 E-5	$3^+, 3^-$		4
AF8		SINGLE FAULTS TO EVENT 3B-1			1.4 E-5			
	CIRCUIT BKR 3340	PREMATURE TRANSFER (OPEN)	1.0 E-6	14	1.4 E-5	$3^+, 3^-$		4
		MCC BUS 3B UNAVAILABLE			5.6 E-5			
AF2		SINGLE FAULTS, 4160V BUS B			1.4 E-5			
	CIRCUIT BKR 3206	PREMATURE TRANSFER (OPEN)	1.0 E-6	14	1.4 E-5	$3^+, 3^-$		4
AF5		MCC BUS 3B SINGLE FAULTS			4.2 E-5			
	TRANSFORMER 3B	SAFEGUARD AUX. TRANSFORMER 3B SHORTS	1.0 E-6	4	4.0 E-6	$3^+, 3^-$		4
	TRANSFORMER 3B	FAILS TO OPERATE	1.0 E-6	10	1.0 E-5	$3^+, 3^-$		5
	CIRCUIT BKR 3310	PREMATURE TRANSFER (OPEN)	1.0 E-5	14	1.4 E-5	$3^+, 3^-$		4
	CIRCUIT BKR 3220	PREMATURE TRANSFER (OPEN)	1.0 E-6	14	1.4 E-5	$3^+, 3^-$		4
					Σ=4.2 E-5			
AF10		SINGLE FAULTS TO EVENT 3B-2			1.4 E-5			
	CIRCUIT BKR 3350	PREMATURE TRANSFER (OPEN)	1.0 E-6	14	1.4 E-5	$3^+, 3^-$		4

Table D.7 (5/5) Event "MCC-3AB" Quantification (Non-LOSP)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
AF9A		SINGLE FAULTS TO BUS 3A			1.4 E-5			
	CIRCUIT BKR 3361	PREMATURE TRANSFER	1.0 E-6	14	1.4 E-5	3^+, 3^-		4
AF9B		SINGLE FAULTS TO BUS 3B, AND OPERATOR FAILS TO TRANSFER			1.0 E-2			
	CIRCUIT BKR 3360	PREMATURE TRANSFER	1.0 E-6	14	1.4 E-5	3^+, 3^-		4
	SWITCH MCC3A-B	TRANSFER SWITCH FAILS TO CLOSE	D		1.0 E-5	3^+, 3^-		
	OPERATOR	FAILS TO TRANSFER	D		1.0 E-2	3^+, 10^-	0	
					Σ=1.0 E-2			

BEST DOCUMENT AVAILABLE

Table D.7 AC Power

QUANTIFICATION TABLES

NOTES

1 Times for the injection phase can vary from 0.5 to 10 hours depending on LOCA size. A fault duration time of 10 hours was conservatively chosen for the injection time.

2 This fault was not evaluated but was assumed to be of lower probability than other faults in this gate.

3 Testing occurs approximately three times a month with an average duration of three hours. Testing itself does not remove the diesel from service; however, loss of offsite power during testing would present the diesel with a full-load reject situation, which is assumed to trip the diesel off-line. Unscheduled maintenance occurs approximately two times per year with an average duration of 15 hours.

4 Technical Specifications require the plant to go to hot shutdown within eight hours after loss of AC-bus. This fault was assessed as an unavailability of a failed equipment.

5 Ten hours fault duration time was conservatively assumed to represent the injection phase.

6 Availability for unit is defined as portion of time plant is producing power or in spinning reserve. Plant records show this to be about 80% of the time for CR-1 and CR-2.

7 Unit has experienced two opportunities to run back on loss of offsite power, and has been successful once. Hence, the probability of a successful runback was estimated as 0.5.

8 See DC Power Distribution System quantification tables for LOSP case.

Table D.8 AC Power Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
A1	1.0 E-3
A2	0.36
A6	0.2
A7	0.5
A8	0.2
A9	0.5
A3	6.1 E-2
AX1	3.2 E-3
DCA	3.2 E-3
AM1	1.6 E-2
A4	1.0 E-3
A5	6.2 E-2
AX2	3.2 E-3
DCB	3.2 E-3
AM2	1.6 E-2
AF6	1.4 E-5
MCC3A	5.6 E-5
AF1	1.4 E-5
AF4	4.2 E-5
AF7	1.4 E-5
AF8	1.4 E-5
MCC3B	5.6 E-5
AF2	1.4 E-5
AF5	4.2 E-5
AF10	1.4 E-5
AF9A	1.4 E-5
AF9B	1.0 E-2

[redacted]

APPENDIX E

NUCLEAR SERVICES CLOSED CYCLE COOLING SYSTEM

APPENDIX E NUCLEAR SERVICES CLOSED CYCLE COOLING SYSTEM (NSCCCS)

E.1 SYSTEM DESCRIPTION AND OPERATION

The Nuclear Services Closed Cycle Cooling System (NSCCCS) is a safety related system which provides cooling to various nuclear oriented equipment during normal and emergency operation. Typical loads during emergency operation are makeup pumps MUP-1A and 1B (part of the HPI system), reactor building fan assembly cooling coils, ventilation fan motor coolers, and control complex chillers. In addition, the NSCCCS provides cooling to its own pumps and to the pumps of the Nuclear Services Seawater System (NSSWS). The NSSWS is part of the Raw Seawater System and serves as a heat sink for the NSCCCS.

E.1.1 SYSTEM DESCRIPTION

The NSCCCS, shown in Figure E.1, is a single closed loop system that removes heat from the containment atmosphere and component heat. The once-through Nuclear Services Seawater System (NSSWS), shown in Figure E.2 takes suction from the seawater sump, removes heat from the closed cycle loop, and discharges into the seawater discharge canal. Component design information for the major components in these systems is given in Table E.1

The NSCCCS consists of one normally operating pump, SWP-1C, and two 100% rated emergency pumps, SWP-1A and -1B. The non-safety pump SWP-1C is sized to supply the normal flowrate of 6900 gpm — which is insufficient for emergency operation. The emergency flow rate of 11,000 gpm can be delivered by each of the two emergency pumps. SWP-1A and -1B each consists of two half-sized pumps driven by a single shaft. Each of the five pumps has a check valve in the discharge line and a manual blocking valve on either side. The pumps discharge into a single header. The main line is 18 inches in diameter. At each heat load center, smaller lines supply water to the individual components. Most of the major heat load centers can be isolated by manual block valves.

The heat absorbed by the NSCCCS is transferred to the NSSWS by a bank of four one-third capacity heat exchangers (HE). Three operable heat exchangers are required for both emergency and normal operation. The HE's have no automatic isolation capability. Each HE has an inlet and outlet manual blocking valve on both the seawater side and the primary side. The heat exchangers are of the shell and tube type, with seawater flow through the tubes. The NSCCCS emergency flow rate of 3700 gpm per HE results in a heat rejection rate of 92×10^6 BTU/hr per heat exchanger. Outlet temperature of the HE's is 105°F under emergency operation.

The NSSWS has one non-safety pump for normal operation and two 100% redundant emergency pumps. The non-safety pump RWP-1 is sized for a normal flow rate of 10,800 gpm and cannot supply the emergency flow rate of 14,100 gpm (4700 gpm/HE). Each pump is provided with a check valve on the discharge side and with manual blocking valves on both sides for isolation purposes. The inlet temperature is determined by the Gulf of Mexico. Technical Specification prohibits operation if the inlet temperature rises above 105°F. For environmental reasons, the temperature rise through the heat exchanger is limited to a maximum of 6°F. Seawater flows by gravity from the intake canal to the seawater sump, through 48 inch pipes. The emergency pumps are installed in separate compartments of the seawater sump to allow the isolation of either compartment for service without disabling the system.

The pump motors are cooled by the NSCCCS. The bearing is cooled by the domestic water supply. If that system fails, the demineralized water supply can provide water through the domestic water lines. If both of these systems fail, seawater will back into the bearing. This provides adequate cooling although it is not desirable for long-term cooling because of corrosion considerations.

The NSSWS has no MOV's or remotely operated valves. There are no locked valves in the system. Manual valves are locally indicated.

The pumps in the NSCCCS and NSSWS are powered from the 4160V ESF buses.

E.1.2 SYSTEM OPERATION

The NSCCCS and the NSSWS are continuously operating systems required for normal plant operation. Upon ESAS, the nonessential loads on the NSCCCS are isolated by closing the inlet and outlet valves in the appropriate line. These loads are primarily isolated to protect against missile damage to the NSCCCS and subsequent drainage of the system. The loads involved are not active during post-LOCA time periods. The ESAS will start both NSCCCS pumps (SWP-1A, -1B) and both Raw Water Pumps (RWP-2A, -2B). Fifteen seconds after either emergency pump in each system starts, the corresponding non-safety pump is tripped.

If one HE is inoperable due to rupture, blockage, or electrolytic erosion/corrosion, the HE-bank can be reconfigured during plant operation by isolating the faulty exchanger on both sides and opening the block valves on both sides of the inactive heat exchanger. The inactive HE is not required to be tested for operability. There is a procedure for freshwater layup on the seawater side to prevent marine growth for long periods of time.

The pumps SWP-1A, -B and RWP-2A, -2B are required to be started once a month (SP-344). The pumps are tested on a two-week staggered basis. Testing of the pumps does not disrupt system service. Technical Specifications require that two emergency pumps be operable in each system. Plant operation can continue for not more than 72 hours if only one emergency pump is available in the NSCCCS or in the NSSWS.

Table E.1

Component Design Information

Nuclear Service Heat Exchangers

Number	4
Type	Shell and Tube
Sea Cocling Water Flow (tubeside), gpm	4700 Emerg; 3600 Normal
Sea Cooling Water Temperature, F	85
Closed Cycle Cooling Water Outlet Temp, F	105 Emerg; 90 Normal
Closed Cycle Cooling Water Flow (shell side), gpm	3700 Emerg; 2300 Normal
Tube Material	90-10 Cu-Ni
Shell Material	Welded Carbon Steel
Channel Material	2% Nickel Cast Iron
Design Pressure, Shell/Tube, psig	200/100
Design Temperature, Shell/Tube, F	180/150
Code/Seismic Class	ASME Section VIII/I
Duty Btu/h	92 X 10^6 Emergency

Nuclear Service Seawater Pumps

Number	2 Emerg; 1 Normal
Flow, gpm	14,100 Emerg; 10,800 Normal
Design Head, ft	144 Emerg; 98 Normal
Design Pressure, psig	100
Design Temperature, F	109
Seismic Class	I

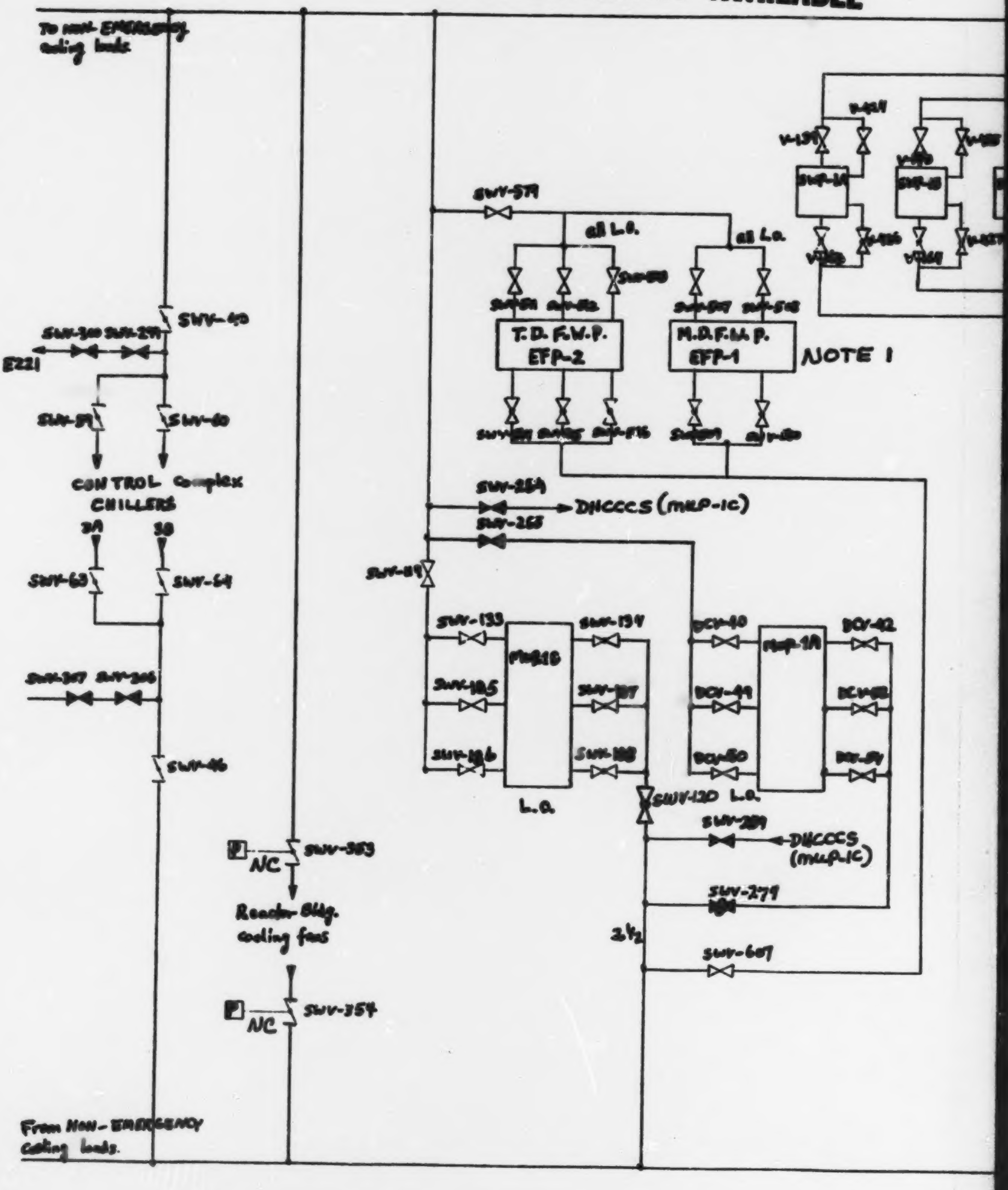
Nuclear Service Closed Cycle Cooling Pumps

Number	2 Emerg; 1 Normal
Flow, gpm	11,000 Emerg; 6,900 Normal
Design Head, ft	190 Emerg; 110 Normal
Design Pressure, psig	200
Design Temperature, F	135
Seismic Class	I

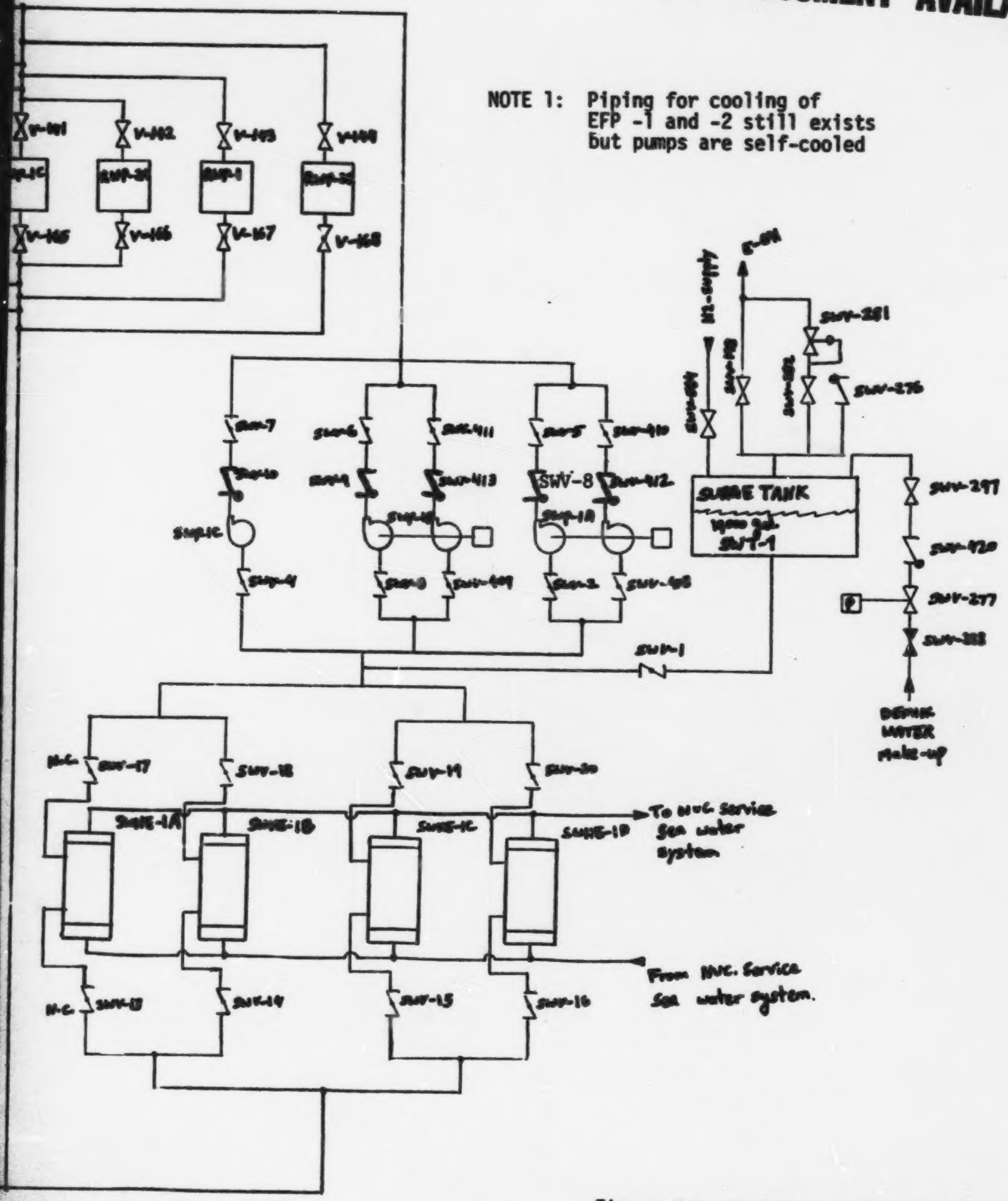
Nuclear Service Closed Cycle Surge Tank

Number	1
Capacity, gal.	10,000
Design Temperature, F	135
Design Pressure, psig	100
Material	Carbon Steel, ASTM
Code/Seismic Class	ASME Section VIII/I

BEST DOCUMENT AVAILABLE


To non-EMERGENCY cooling loads
SWV-40
SWV-300
SWV-299
E221
SWV-59
SWV-60
CONTROL complex CHILLERS
3A
3B
SWV-63
SWV-64
SWV-307
SWV-306
SWV-46
NC
SWV-353
Reactor Bldg. cooling fans
NC
SWV-354
From NON-EMERGENCY cooling loads.
SWV-579
all L.O.
all L.O.
V-421
V-139
SWV-580
SWV-582
SWV-517
SWV-518
T.D. F.W.P.
EFP-2
M.D.F.W.P.
EFP-1
NOTE 1
SWV-516
SWV-264
DHCCCS (MUP-1C)
SWV-265
SWV-119
SWV-133
SWV-134
SWV-135
SWV-137
SWV-136
SWV-138
L.O.
SWV-120
L.O.
DCV-40
MUP-1A
DCV-42
DCV-49
DCV-50
SWV-289
DHCCCS (MUP-1C)
SWV-279
2½
SWV-607

BEST DOCUMENT AVAILABLE



NOTE 1: Piping for cooling of
EFP -1 and -2 still exists
but pumps are self-cooled

V-161
V-162
V-163
V-164
RWP-1C
RWP-2A
RWP-1
RWP-2B
V-165
V-166
V-167
V-168
SWV-7
SWV-10
SWP-1C
SWV-4
SWV-6
SWV-9
SWV-411
SWV-413
SWP-1B
SWV-3
SWV-409
SWV-5
SWV-8
SWV-410
SWV-412
SWP-1A
SWV-2
SWV-408
SWV-1
NI-Supply
SWV-284
SWV-278
SWV-282
SWV-281
SWV-276
SURGE TANK
10,000 gal.
SWT-1
SWV-297
SWV-420
SWV-277
SWV-288
DEMIN
WATER
Make-up
N.C.
SWV-17
SWV-18
SWV-19
SWV-20
SWHE-1A
SWHE-1B
SWHE-1C
SWHE-1D
To NUC Service
Sea water
system
From NUC. Service
Sea water system.
N.C.
SWV-13
SWV-14
SWV-15
SWV-16

Figure E.1 Nuclear Services Closed Cycle
Cooling System Schematic Diagram

BEST DOCUMENT AVAILABLE

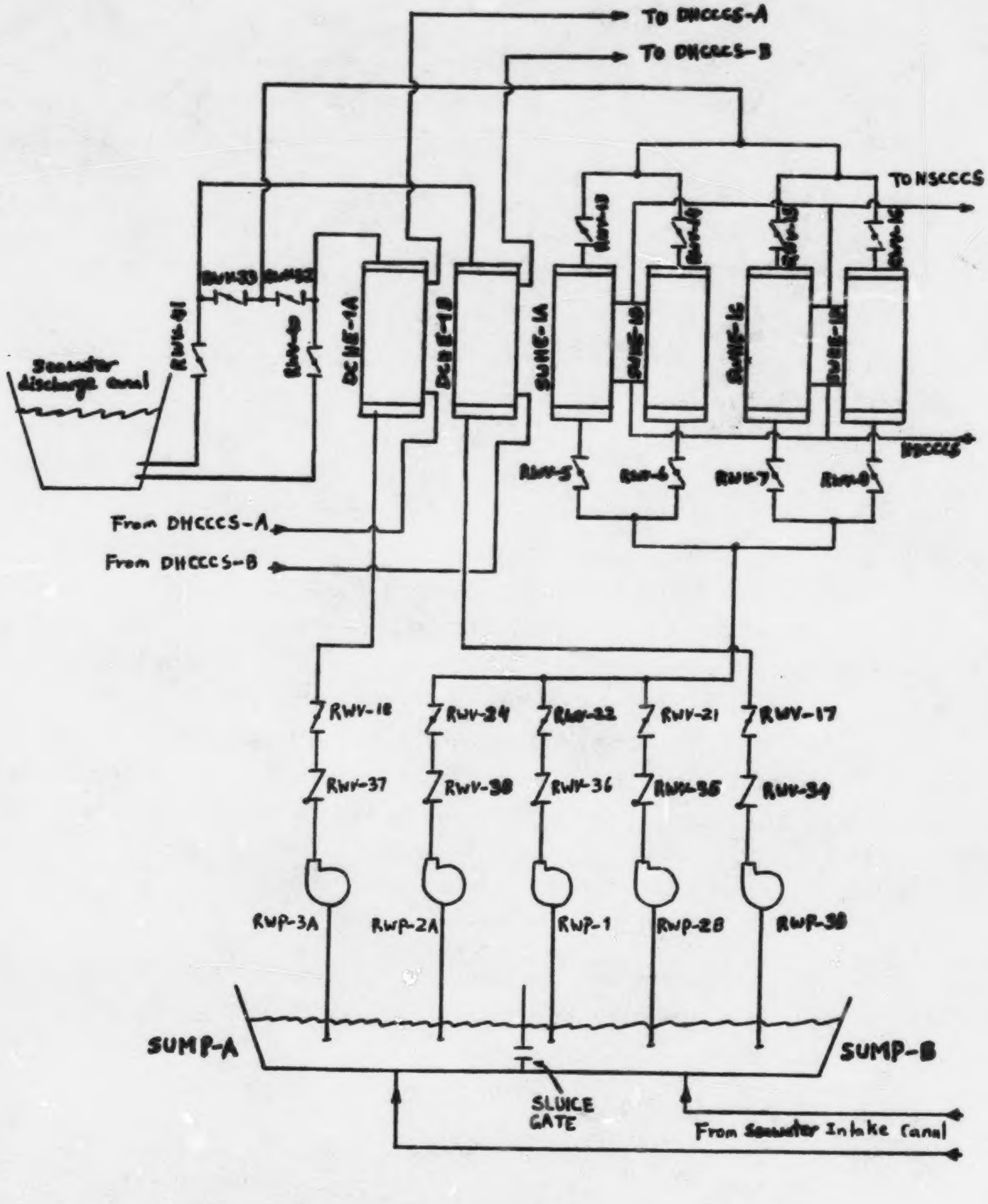

To DHCCCS-A
To DHCCCS-B
TO NSCCCS
Seawater discharge canal
RWV-31
RWV-33
RWV-32
DCHE-1A
DCHE-1B
SWHE-1A
SWHE-1B
SWHE-1C
SWHE-1D
NSCCCS
RWV-5
RWV-6
RWV-7
RWV-8
From DHCCCS-A
From DHCCCS-B
RWV-18
RWV-24
RWV-22
RWV-21
RWV-17
RWV-37
RWV-38
RWV-36
RWV-35
RWV-34
RWP-3A
RWP-2A
RWP-1
RWP-2B
RWP-3B
SUMP-A
SUMP-B
SLUICE GATE
From Seawater Intake Canal

Figure E.2 Nuclear Services Seawater System Schematic Diagram

E.2 SYSTEM SIMPLIFIED FAULT TREE

Detailed fault trees were initially drawn for both the NSCCCS and the NSSWS. The detailed trees were simplified and combined in a series of intermediate steps to arrive at a single simplified tree. The top event for this fault tree is defined as:

> NSCCCS Failure - failure of the NSCCCS to produce rated emergency flow at the rated temperature and head at the pump discharge header.

Because of the fact that several pump operability states are possible, several separate simplified fault trees were constructed to describe these cases. Figure E.3 is the simplified fault tree for the normally operating configuration, with the non-emergency pumps (SWP-1C and RWP-1) in service. Figure E.4 is the simplified fault tree for one of the four possible cases where both non-emergency pumps are not in service and one emergency pump is running in each system. Figures E.5 and E.6 are the simplified fault trees for two of the four possible cases where one system is operating with an emergency pump in service and the other system is operating with a normal (non-emergency) pump in service. The evaluation was performed only for the normally operating configuration (the tree shown in Figure E.3), which is the most conservative case. Since it was subsequently found that this system is not a dominant contributor to any of the dominant sequences, it was unnecessary to evaluate the other cases.

MAJOR ASSUMPTIONS

The assumptions used to construct the detailed fault trees for NSCCCS and NSSWS before they were combined in the simplified trees are listed in the following two subsections.

NSCCCS - Fault Tree

1. The NSCCCS is normally in operation. Correct valve alignment in the major flow lines is assumed to exist at the time of an ESAS signal. For the purpose of this analysis it is assumed that pump SWP-1C is running (see also Section E.1). The emergency pumps are not normally in operation. Therefore, mispositioning of the block valves in the emergency pump lines is addressed.

2. If pressure is lost in the surge tank, the pumps will not cavitate.

3. The normal nuclear service pump can not supply the emergency flow rate.

4. Failure to isolate nonessential loads from the NSCCCS is not necessarily a failure (these loads being the CRDM coolers, RCP motor coolers, waste evaporators, etc.). The loads are not isolated for heat load or hydraulic considerations. Isolation is desirable because the components are not missile protected and are located in LOCA-missile susceptible areas.

5. SWP-1A and 1B and the associated check valves (SWV-9, 413, 8, 412) are each tested once a month on a staggered basis.

6. The pumps are self-cooled. Blockage of the NSCCCS pump motor cooling lines when these pumps are in service was not considered. Blockage of these lines was considered for standby pumps.

7. The system does not require reconfiguration for testing.

8. Components, lines, and valves that were considered to be insignificant were omitted from the fault trees.

NSSWS - Fault Tree

1. The system is normally in operation. Correct valve alignment in the major flow lines is assumed to exist at the time of an ESAS signal. For the purpose of this analysis it is assumed that pump RWP-1 is running. The emergency pumps are not normally in operation. Therefore, mispositioning of the block valves in the emergency pump lines is addressed.

2. RWP-2A and 2B are cooled by the NSCCCS. If the motor loses cooling, it is assumed to fail immediately. Loss of cooling to the bearing is not significant for this study. The bearing pot is supplied by three sources. Cooling is accomplished by circulation of water through the bearing pot. The primary source of water is the domestic water system. The demineralized water system backs up the domestic water supply system. If both of these systems fail, seawater will back into the bearing. This provides adequate cooling. It is not done on a permanent basis because it is undesirable from a corrosion standpoint.

3. The Auxiliary Building contains the two DHCCCS pumps, the four NSCCCS heat exchangers, the two DHCCCS heat exchangers, and the three surge tanks. Common causative damage events could result in significant flooding of the room. This is a single fault for both RWP-2A and 2B. However, the pump room is large and is equipped with a sump pump.

4. Pump cavitation was considered unlikely enough to be ignored.

5. The normal seawater service pump cannot supply the emergency flow rate.

6. Pump and check valve testing do not cause the system to be unavailable.

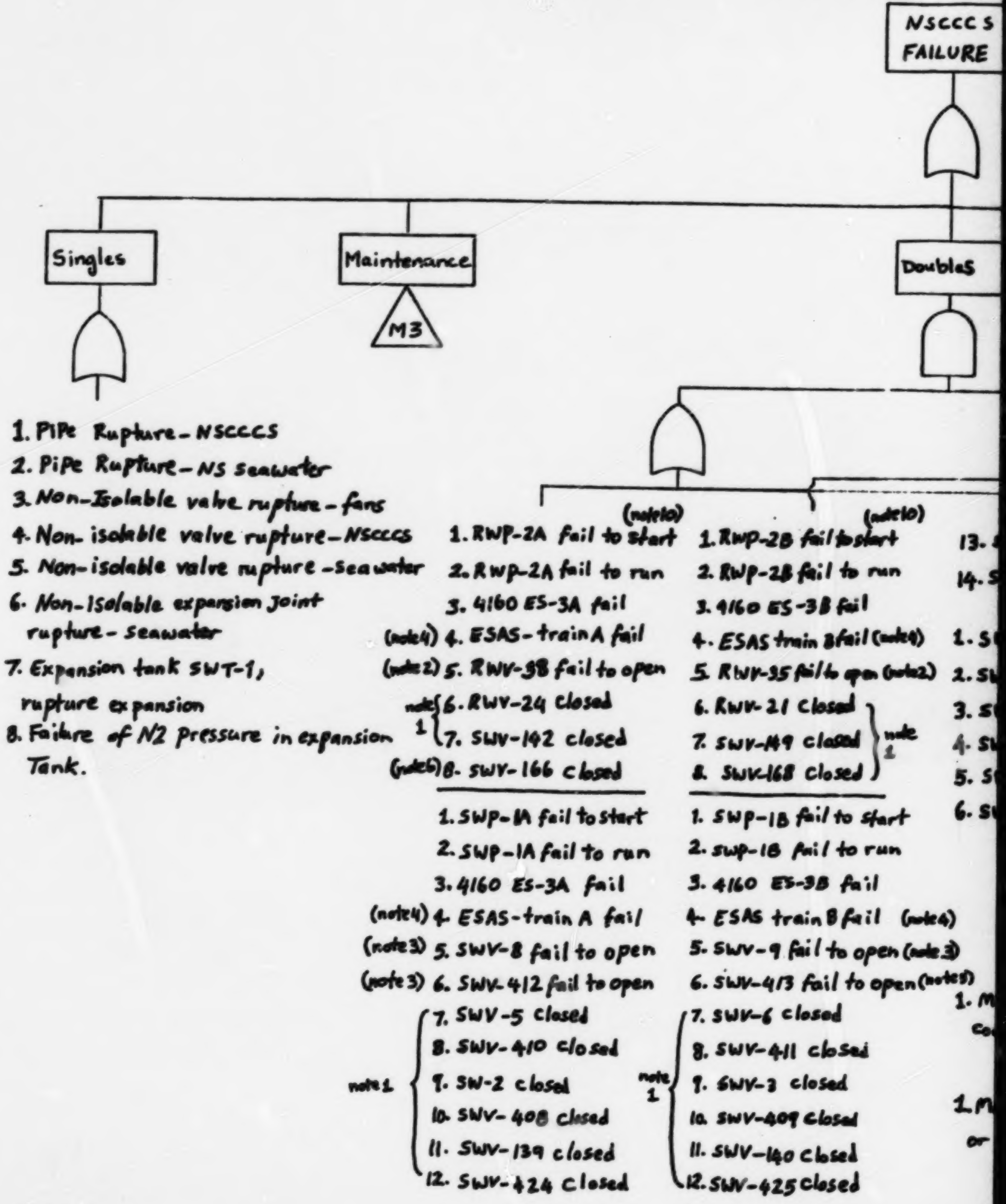
7. It was assumed the intake canal never goes dry while the plant is operating. T.S. 3.4.7.5 limits the bottom of the canal to EL 74 and the minimum water level to EL 81. T.S. 4.7.5.1 requires the inlet water temperature and water level to be checked every 24 hours. It was further assumed the seawater sump never goes dry. Either section may be taken out of service for maintenance, one at a time. There is a 48" pipe which gravity feeds the seawater sump from the intake structure. A separate pipe goes from the intake structure to each sump. A sluice gate also connects the two sumps. The canal is wide enough to preclude blockage by shipwreck. There are large grates on the intake structure which remove trash, seaweed, flotsam, and jetsam from the seawater. It was assumed that blockage of these grates to the extent that they block flow is not possible.

8. OP-416 contains a procedure for the lay-up of the seawater side of the inactive NSCCCS heat exchanger (SWHE) to prevent marine growth. This basically is a gravity drain and flush with domestic water. It involves opening and closing of drain valves, vent valves, and fill valves. Because these lines are very small, discharge rates would be very small if a valve was inadvertently left in the wrong position. For this reason, improper filling procedure was not considered a possible fault.

9. Due to its nature, the seawater system is exposed to a very corrosive-marine growth environment. Equipment in the system was therefore assigned higher failure rates (an order of magnitude) than would have been the case for equipment operating in freshwater. Failure (plugging, blockage, marine-encrustation) of equipment in the dormant state was also considered. However, plugging and blockage of equipment while in operation was not considered likely.

10. Components, lines, and valves that were considered to be insignificant were omitted from the fault trees.

BEST DOCUMENT AVAILABLE



1. PiPe Rupture-NSCCCS
2. Pipe Rupture-NS Seawater
3. Non-Isolable valve rupture-fans
4. Non-isolable valve rupture-NSCCCS
5. Non-isolable valve rupture-Seawater
6. Non-Isolable expansion Joint rupture-Seawater
7. Expansion tank SWT-1, rupture expansion
8. Failure of N2 pressure in expansion Tank.

(note10)
1. RWP-2A fail to start
2. RWP-2A fail to run
3. 4160 ES-3A fail
(note4) 4. ESAS-train A fail
(note2) 5. RWV-38 fail to open
note 1 { 6. RWV-24 Closed
note 1 { 7. SWV-142 closed
(note6) 8. SWV-166 Closed

---

1. SWP-1A fail to start
2. SWP-1A fail to run
3. 4160 ES-3A fail
(note4) 4. ESAS-train A fail
(note3) 5. SWV-8 fail to open
(note3) 6. SWV-412 fail to open
note1 { 7. SWV-5 Closed
note1 { 8. SWV-410 closed
note1 { 9. SW-2 closed
note1 { 10. SWV-408 closed
note1 { 11. SWV-139 closed
note1 { 12. SWV-424 Closed

(note10)
1. RWP-2B fail to start
2. RWP-2B fail to run
3. 4160 ES-3B fail
4. ESAS train B fail (note4)
5. RWV-35 fail to open (note2)
6. RWV-21 Closed } note 1
7. SWV-149 closed } note 1
8. SWV-168 Closed } note 1

---

1. SWP-1B fail to start
2. SWP-1B fail to run
3. 4160 ES-3B fail
4. ESAS train B fail (note4)
5. SWV-9 fail to open (note3)
6. SWV-413 fail to open (note5)
note 1 { 7. SWV-6 closed
note 1 { 8. SWV-411 closed
note 1 { 9. SWV-3 closed
note 1 { 10. SWV-409 Closed
note 1 { 11. SWV-140 Closed
note 1 { 12. SWV-425 Closed

13.
14.

1.
2.
3.
4.
5.
6.

1.

1.
or

BEST DOCUMENT AVAILABLE

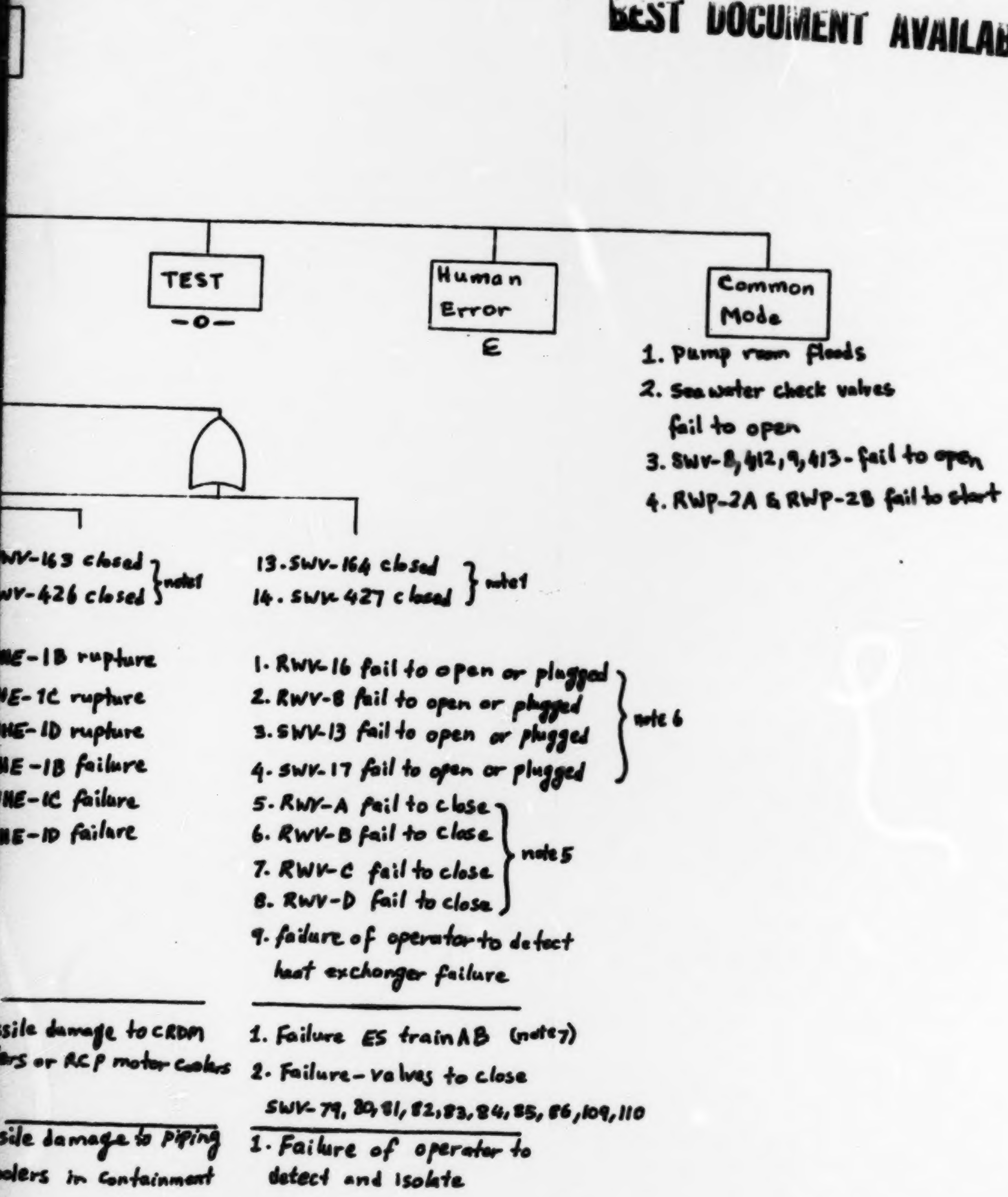

TEST
-O-
Human Error
E
Common Mode
1. Pump room floods
2. Sea water check valves fail to open
3. SWV-8, 412, 9, 413 - fail to open
4. RWP-2A & RWP-2B fail to start
WV-163 closed
WV-426 closed
note1
13. SWV-164 closed
14. SWV-427 closed
note1
HE-1B rupture
HE-1C rupture
HE-1D rupture
HE-1B failure
HE-1C failure
HE-1D failure
1. RWV-16 fail to open or plugged
2. RWV-8 fail to open or plugged
3. SWV-13 fail to open or plugged
4. SWV-17 fail to open or plugged
note 6
5. RWV-A fail to close
6. RWV-B fail to close
7. RWV-C fail to close
8. RWV-D fail to close
note 5
9. failure of operator to detect heat exchanger failure
ssile damage to CRDM
lers or RCP motor coolers
1. Failure ES train AB (note 7)
2. Failure - valves to close SWV-79, 80, 81, 82, 83, 84, 85, 86, 109, 110
ssile damage to piping
oolers in containment
1. Failure of operator to detect and isolate

Figure E.3 (1/2) Simplified Fault Tree - NSCCCS SWP-1C, RWP-1 Operating (Normal System Configuration)

BEST DOCUMENT AVAILABLE

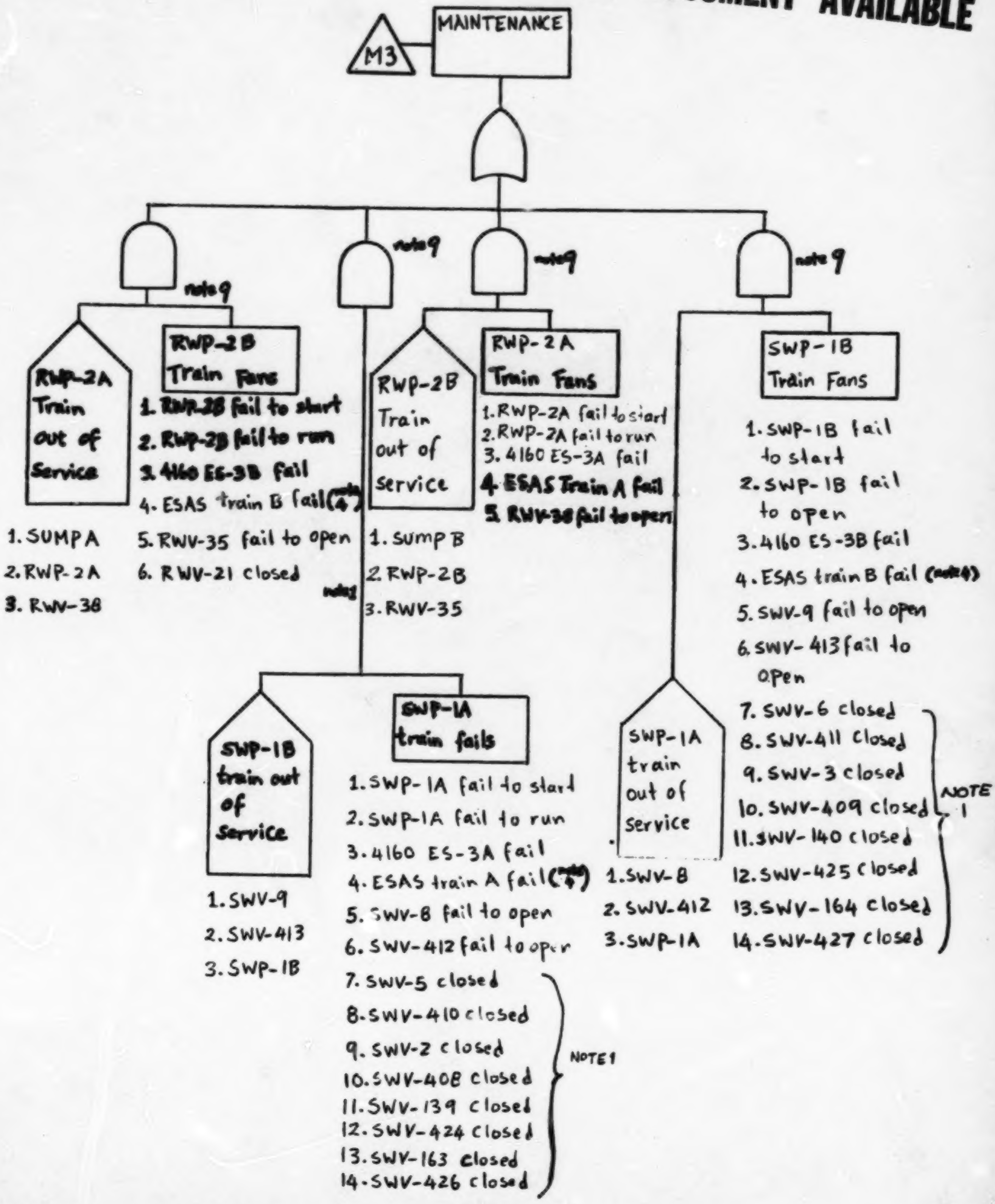
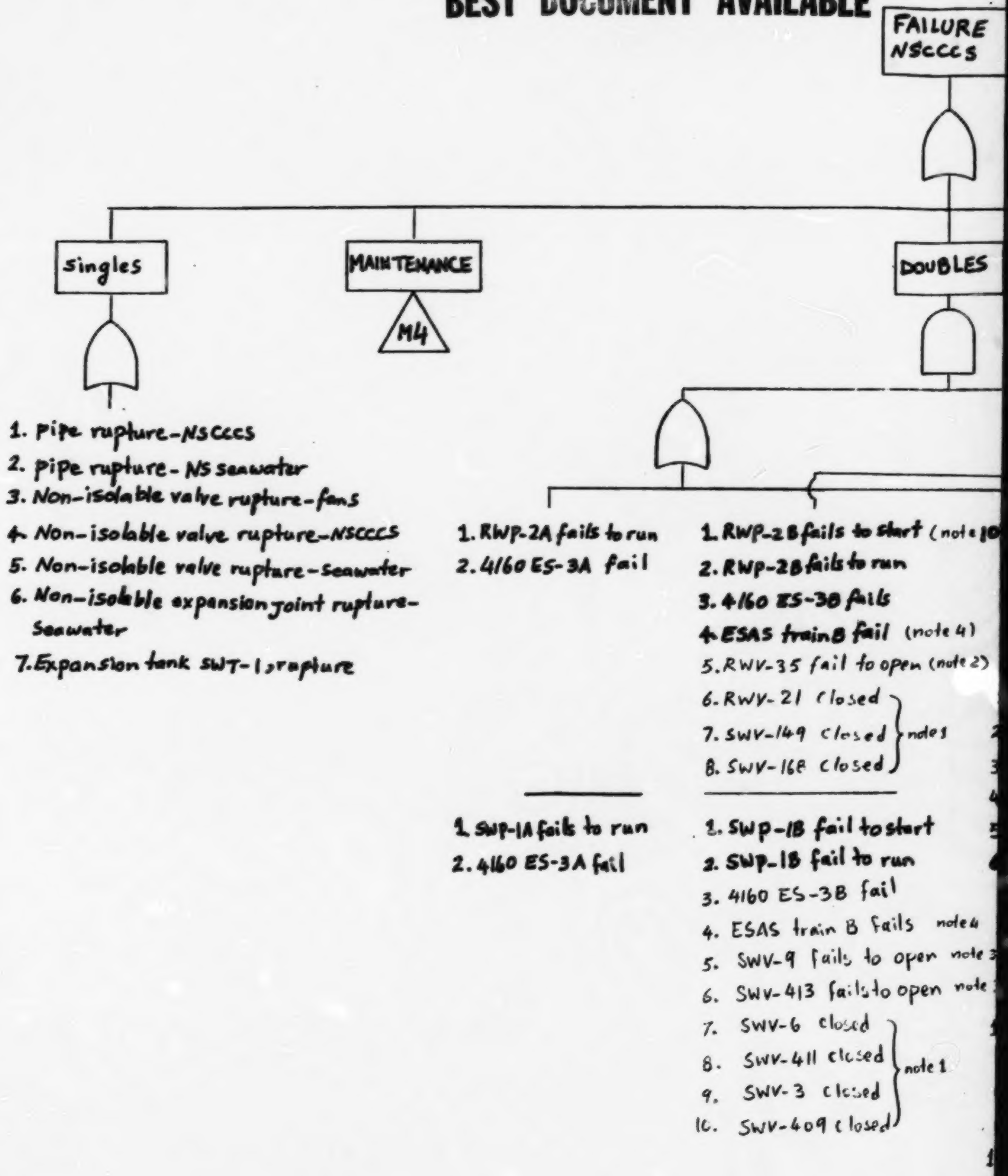

M3
MAINTENANCE
note 9
note 9
note 9
note 9
RWP-2A Train out of Service
1. SUMP A
2. RWP-2A
3. RWV-38
RWP-2B Train Fans
1. RWP-2B fail to start
2. RWP-2B fail to run
3. 4160 ES-3B fail
4. ESAS train B fail (note 4)
5. RWV-35 fail to open
6. RWV-21 closed
RWP-2B Train out of Service
1. SUMP B
2. RWP-2B
3. RWV-35
note 8
RWP-2A Train Fans
1. RWP-2A fail to start
2. RWP-2A fail to run
3. 4160 ES-3A fail
4. ESAS Train A fail
5. RWV-38 fail to open
SWP-1B Train Fans
1. SWP-1B fail to start
2. SWP-1B fail to open
3. 4160 ES-3B fail
4. ESAS train B fail (note 4)
5. SWV-9 fail to open
6. SWV-413 fail to open
7. SWV-6 closed
8. SWV-411 closed
9. SWV-3 closed
10. SWV-409 closed
11. SWV-140 closed
12. SWV-425 closed
13. SWV-164 closed
14. SWV-427 closed
NOTE 1
SWP-1B train out of Service
1. SWV-9
2. SWV-413
3. SWP-1B
SWP-1A train fails
1. SWP-1A fail to start
2. SWP-1A fail to run
3. 4160 ES-3A fail
4. ESAS train A fail (note 4)
5. SWV-8 fail to open
6. SWV-412 fail to open
7. SWV-5 closed
8. SWV-410 closed
9. SWV-2 closed
10. SWV-408 closed
11. SWV-139 closed
12. SWV-424 closed
13. SWV-163 closed
14. SWV-426 closed
NOTE 1
SWP-1A train out of Service
1. SWV-8
2. SWV-412
3. SWP-1A

Figure E.3 (2/2) Simplified Fault Tree - NSCCCS SWP-1C, RWP-1 Operating (Normal System Configuration)

BEST DOCUMENT AVAILABLE


FAILURE NSCCCS
Singles
MAINTENANCE
M4
DOUBLES
1. Pipe rupture-NSCCCS
2. pipe rupture- NS seawater
3. Non-isolable valve rupture-fans
4. Non-isolable valve rupture-NSCCCS
5. Non-isolable valve rupture-Seawater
6. Non-isolable expansion joint rupture-Seawater
7. Expansion tank SWT-1, rupture
1. RWP-2A fails to run
2. 4160 ES-3A fail
1. RWP-2B fails to start (note
2. RWP-2B fails to run
3. 4160 ES-3B fails
4. ESAS train B fail (note 4)
5. RWV-35 fail to open (note 2)
6. RWV-21 Closed
7. SWV-149 Closed
8. SWV-168 Closed
note 1
1. SWP-1A fails to run
2. 4160 ES-3A fail
1. SWP-1B fail to start
2. SWP-1B fail to run
3. 4160 ES-3B fail
4. ESAS train B fails note 4
5. SWV-9 fails to open note
6. SWV-413 fails to open note
7. SWV-6 closed
8. SWV-411 closed
9. SWV-3 closed
10. SWV-409 closed
note 1

BEST DOCUMENT AVAILABLE

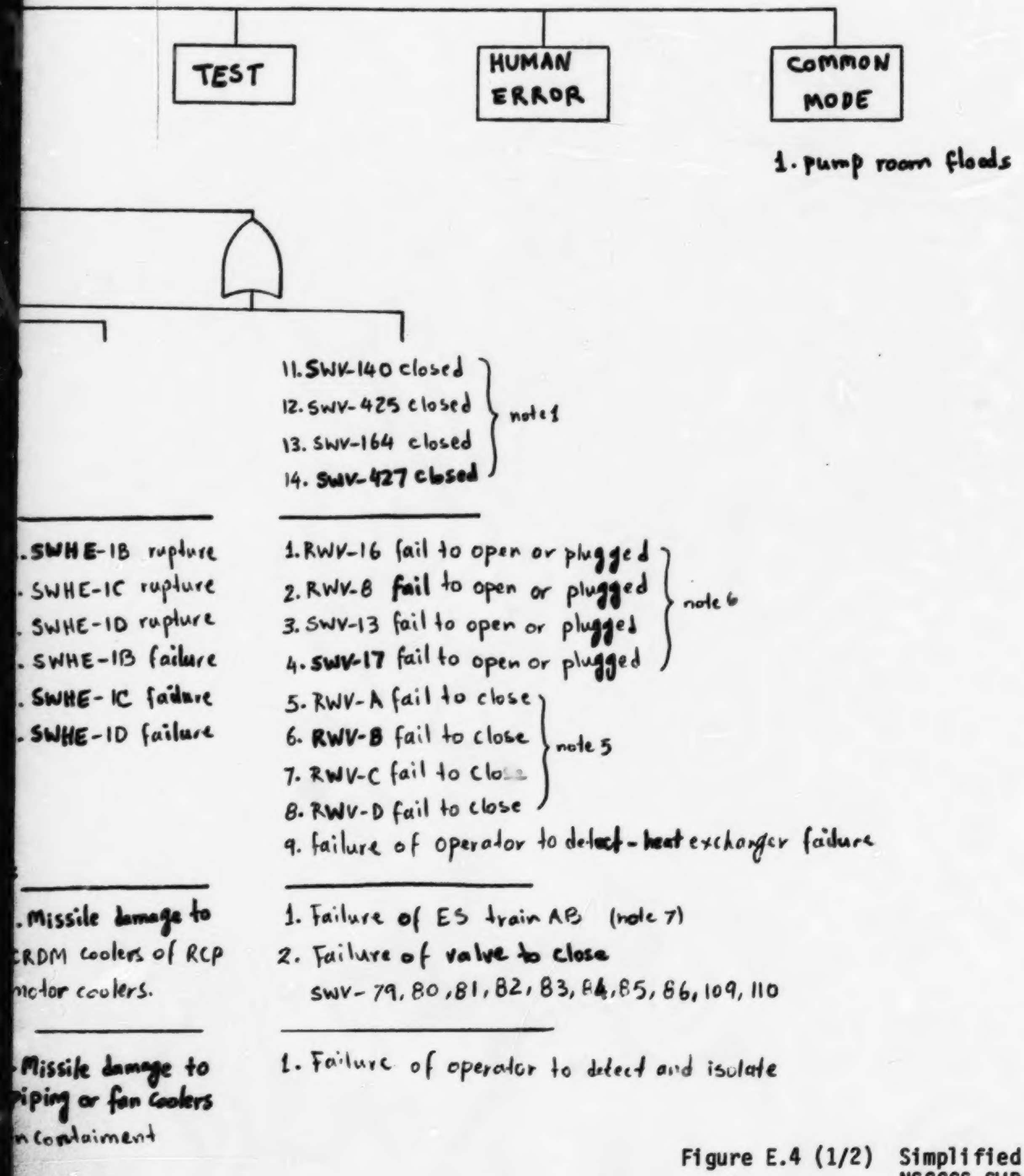
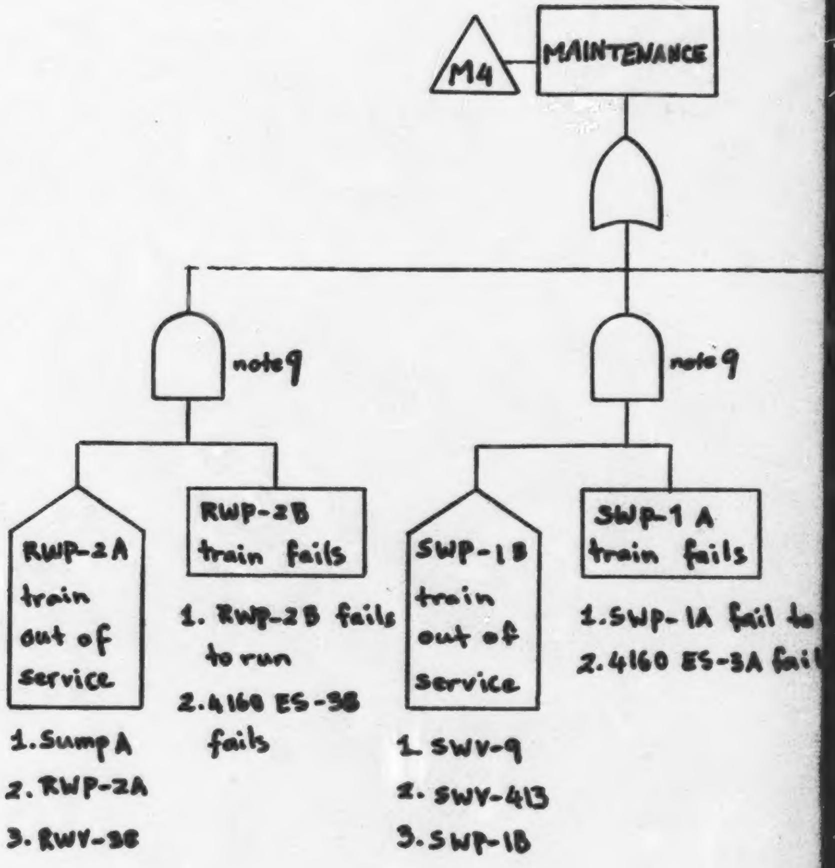

TEST
HUMAN ERROR
COMMON MODE
1. pump room floods
11. SWV-140 closed
12. SWV-425 closed
13. SWV-164 closed
14. SWV-427 closed
note 1
.SWHE-1B rupture
. SWHE-1C rupture
. SWHE-1D rupture
. SWHE-1B failure
. SWHE-1C failure
. SWHE-1D failure
1. RWV-16 fail to open or plugged
2. RWV-8 fail to open or plugged
3. SWV-13 fail to open or plugged
4. SWV-17 fail to open or plugged
note 6
5. RWV-A fail to close
6. RWV-B fail to close
7. RWV-C fail to Close
8. RWV-D fail to close
note 5
9. failure of operator to detect - heat exchanger failure
. Missile damage to
CRDM coolers of RCP
motor coolers.
1. Failure of ES train AB (note 7)
2. Failure of valve to close
SWV-79, 80, 81, 82, 83, 84, 85, 86, 109, 110
Missile damage to
piping or fan coolers
n contaiment
1. Failure of operator to detect and isolate

Figure E.4 (1/2) Simplified Fault Tree - NSCCCS SWP-1A, RWP-2A Operating

BEST DOCUMENT AVAILABLE


M4
MAINTENANCE
note 9
note 9
RWP-2A train out of service
1. Sump A
2. RWP-2A
3. RWV-38
RWP-2B train fails
1. RWP-2B fails to run
2. 4160 ES-3B fails
SWP-1B train out of service
1. SWV-9
2. SWV-413
3. SWP-1B
SWP-1A train fails
1. SWP-1A fail to
2. 4160 ES-3A fail

BEST DOCUMENT AVAILABLE

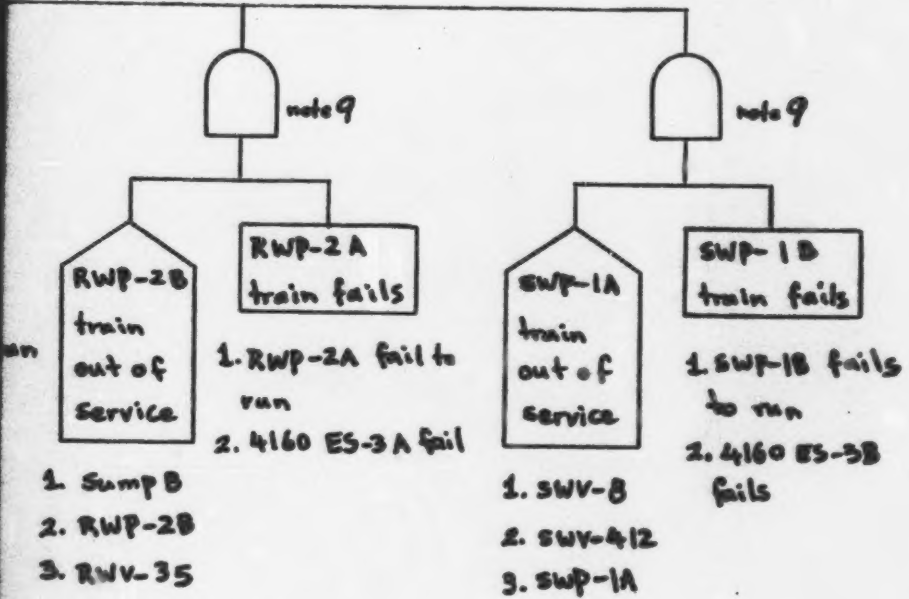
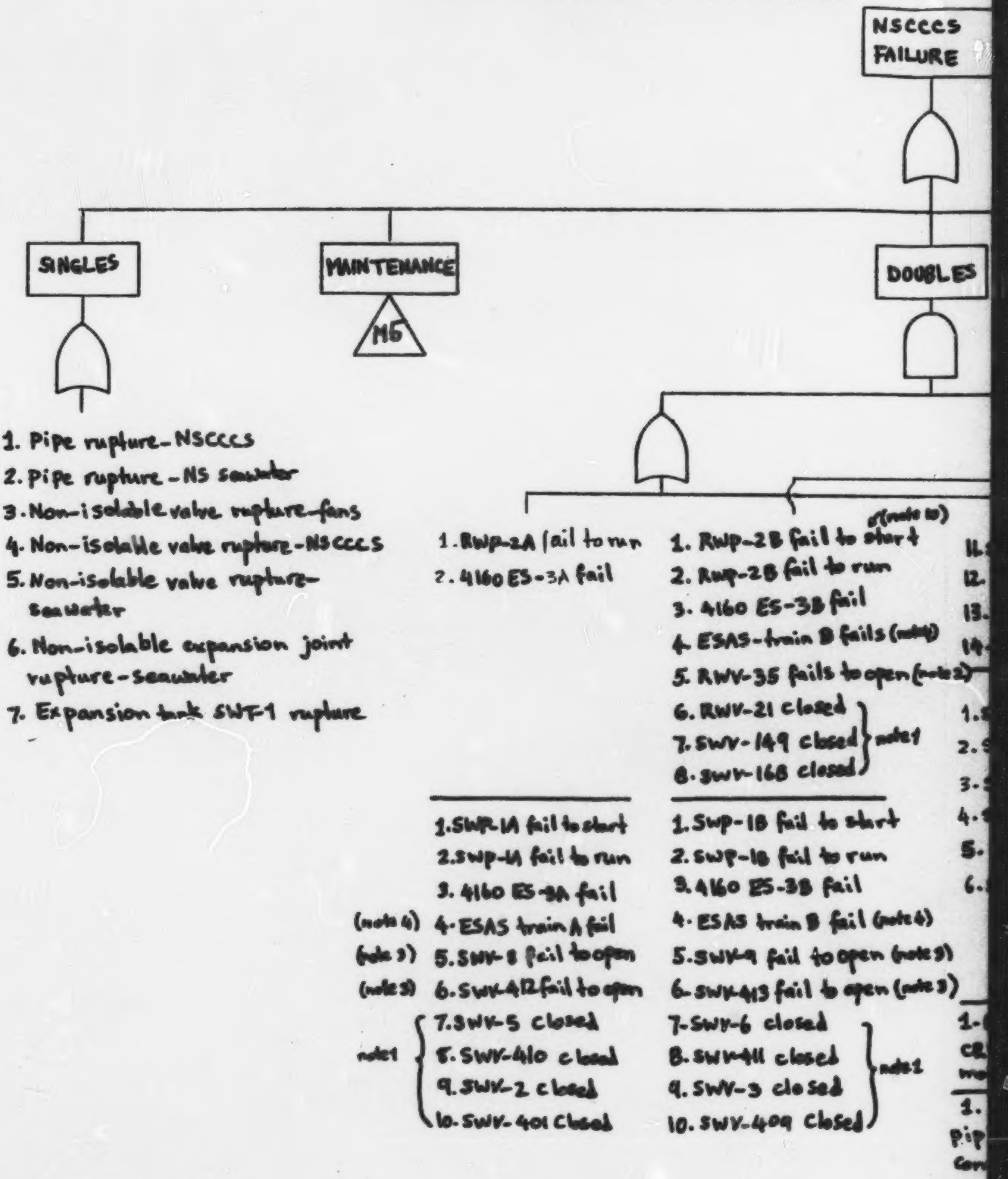

un
note 9
note 9
RWP-2B train out of service
RWP-2A train fails
SWP-1A train out of service
SWP-1B train fails
1. Sump B
2. RWP-2B
3. RWV-35
1. RWP-2A fail to run
2. 4160 ES-3A fail
1. SWV-8
2. SWV-412
3. SWP-1A
1. SWP-1B fails to run
2. 4160 ES-3B fails

Figure E.4 (2/2) Simplified Fault Tree - NSCCCS: SWP-1A, RWP-2A Operating

[redacted]

BEST DOCUMENT AVAILABLE


NSCCCS FAILURE
SINGLES
MAINTENANCE
MS
DOUBLES
1. Pipe rupture-NSCCCS
2. Pipe rupture-NS seawater
3. Non-isolable valve rupture-fans
4. Non-isolable valve rupture-NSCCCS
5. Non-isolable valve rupture-seawater
6. Non-isolable expansion joint rupture-seawater
7. Expansion tank SWT-1 rupture
1. RWP-2A fail to run
2. 4160 ES-3A fail
1. RWP-2B fail to start (note 10)
2. RWP-2B fail to run
3. 4160 ES-3B fail
4. ESAS-train B fails (note 4)
5. RWV-35 fails to open (note 2)
6. RWV-21 closed
7. SWV-149 closed
8. SWV-168 closed
note 1
1. SWP-1A fail to start
2. SWP-1A fail to run
3. 4160 ES-3A fail
(note 4) 4. ESAS train A fail
(note 3) 5. SWV-8 fail to open
(note 3) 6. SWV-412 fail to open
7. SWV-5 closed
8. SWV-410 closed
9. SWV-2 closed
10. SWV-401 Closed
note 1
1. SWP-1B fail to start
2. SWP-1B fail to run
3. 4160 ES-3B fail
4. ESAS train B fail (note 4)
5. SWV-9 fail to open (note 3)
6. SWV-413 fail to open (note 3)
7. SWV-6 closed
8. SWV-411 closed
9. SWV-3 closed
10. SWV-409 Closed
note 1
11.
12.
13.
14.
1.
2.
3.
4.
5.
6.
1-
CR
1.
Pip
Con

BEST DOCUMENT AVAILABLE

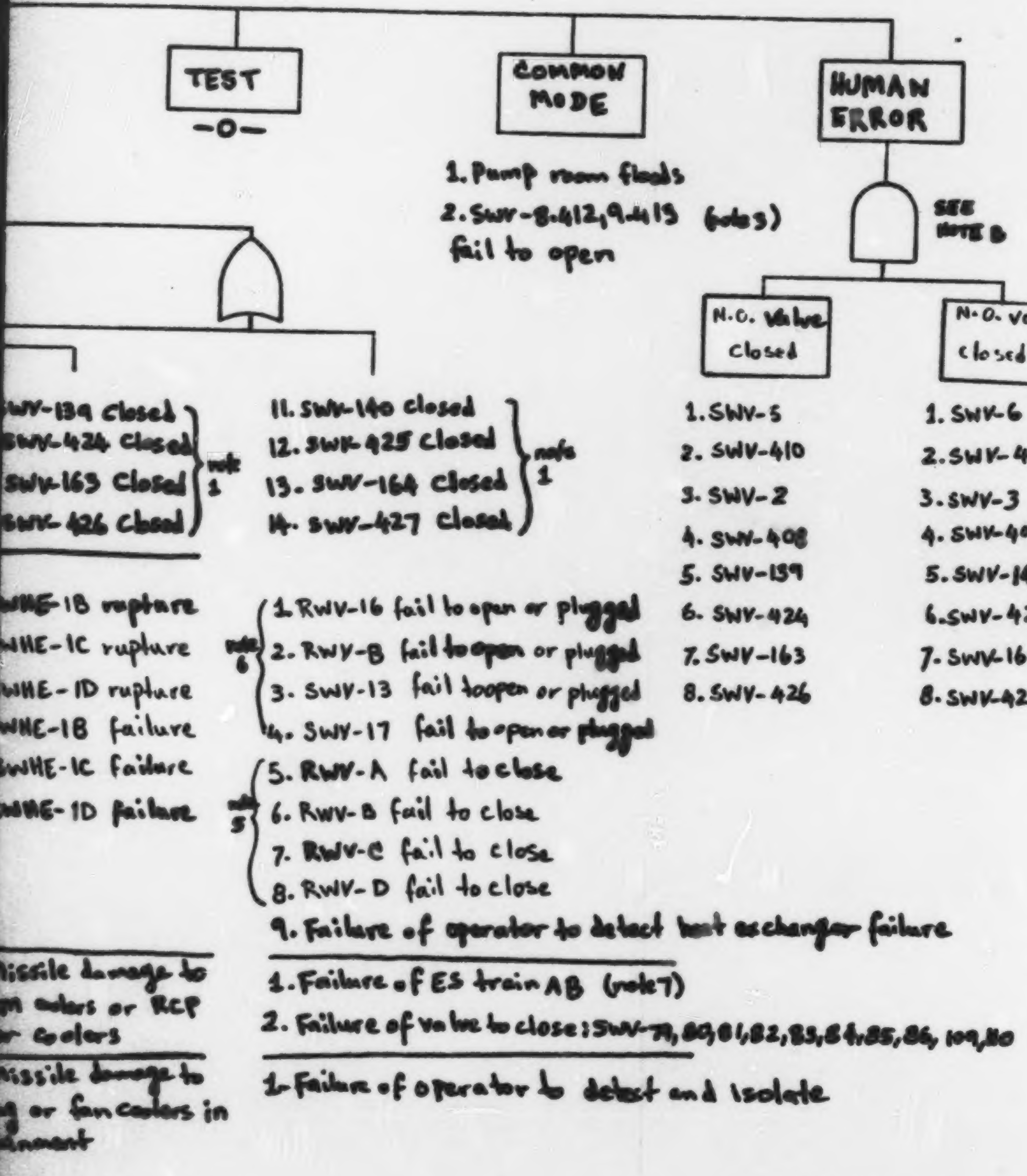
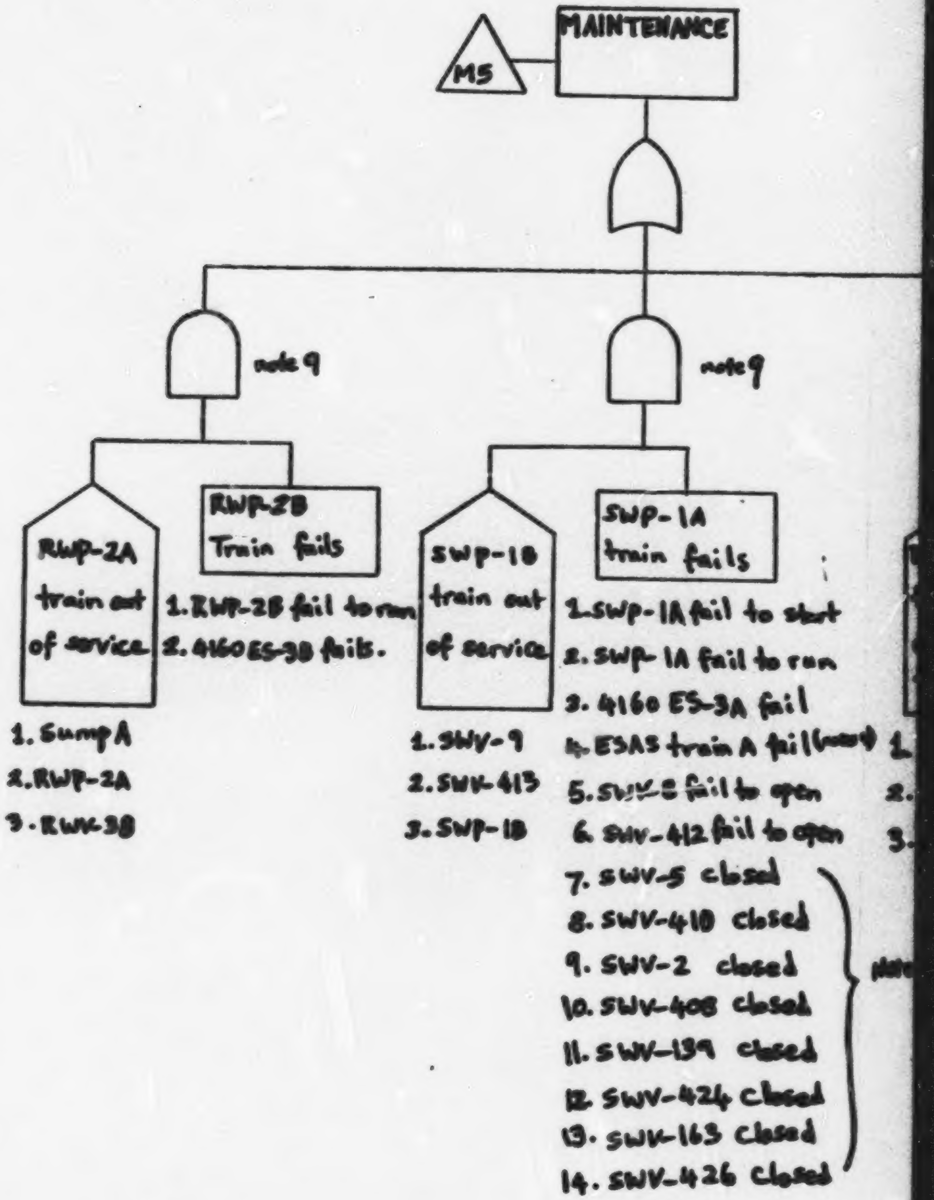

TEST
-O-
COMMON MODE
1. Pump room floods
2. SWV-8.412,9.413 (note 3)
fail to open
HUMAN ERROR
SEE NOTE B
N.O. Valve Closed
N.O. Valve Closed
WV-139 Closed
SWV-424 Closed
SWV-163 Closed
SWV-426 Closed
note 1
11. SWV-140 closed
12. SWV-425 Closed
13. SWV-164 Closed
14. SWV-427 Closed
note 1
1. SWV-5
2. SWV-410
3. SWV-2
4. SWV-408
5. SWV-139
6. SWV-424
7. SWV-163
8. SWV-426
1. SWV-6
2. SWV-411
3. SWV-3
4. SWV-409
5. SWV-140
6. SWV-425
7. SWV-164
8. SWV-427
WHE-1B rupture
WHE-1C rupture
WHE-1D rupture
WHE-1B failure
SWHE-1C failure
WHE-1D failure
note 6
1. RWV-16 fail to open or plugged
2. RWV-B fail to open or plugged
3. SWV-13 fail to open or plugged
4. SWV-17 fail to open or plugged
note 5
5. RWV-A fail to close
6. RWV-B fail to close
7. RWV-C fail to close
8. RWV-D fail to close
9. Failure of operator to detect heat exchanger failure
issile damage to
n coolers or RCP
r coolers
1. Failure of ES train AB (note 7)
2. Failure of valve to close: SWV-79, 80, 81, 82, 83, 84, 85, 86, 109, 110
issile damage to
g or fan coolers in
nment
1. Failure of operator to detect and isolate

Figure E.5 (1/2) Simplified Fault Tree - NSCCCS; SWP-1C, RWP-2A Operating

BEST DOCUMENT AVAILABLE


MAINTENANCE
MS
note 9
note 9
RWP-2A train out of service
1. Sump A
2. RWP-2A
3. RWV-3B
RWP-2B Train fails
1. RWP-2B fail to run
2. 4160 ES-3B fails.
SWP-1B train out of service
1. SWV-9
2. SWV-413
3. SWP-1B
SWP-1A train fails
1. SWP-1A fail to start
2. SWP-1A fail to run
3. 4160 ES-3A fail
4. ESAS train A fail
5. SWV-8 fail to open
6. SWV-412 fail to open
7. SWV-5 closed
8. SWV-410 closed
9. SWV-2 closed
10. SWV-408 closed
11. SWV-139 closed
12. SWV-424 closed
13. SWV-163 closed
14. SWV-426 closed
1.
2.
3.

BEST DOCUMENT AVAILABLE

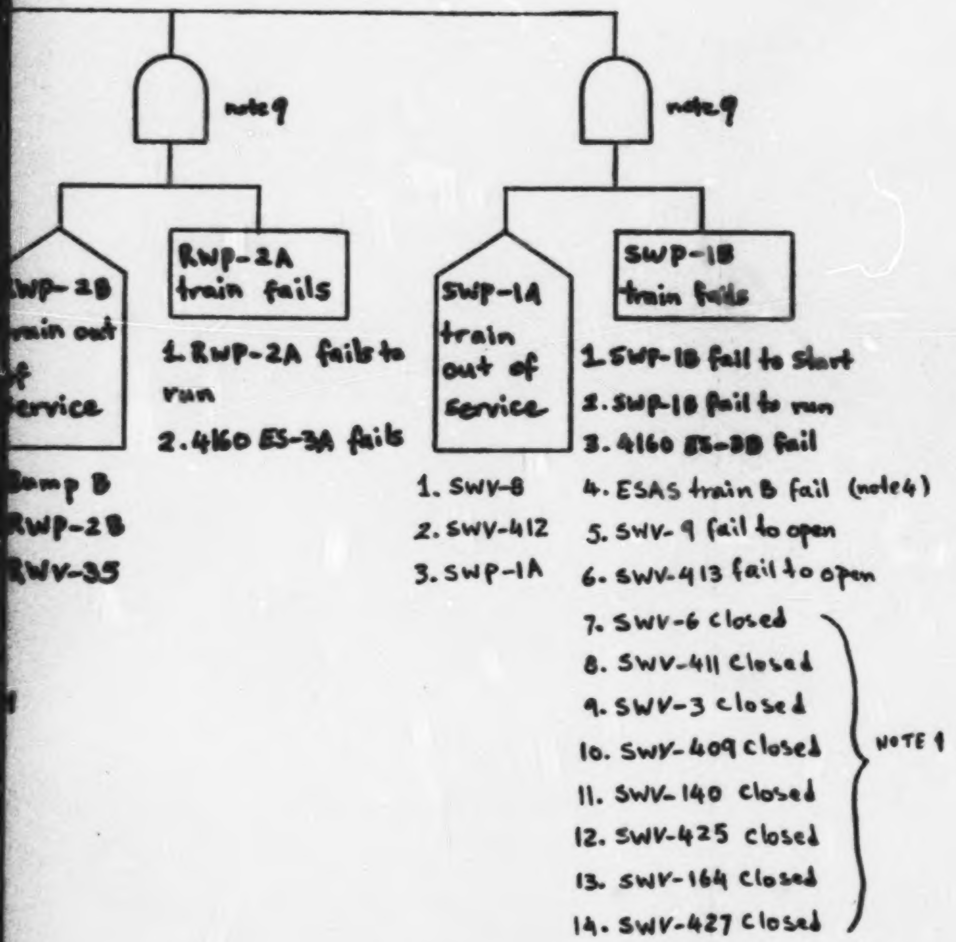
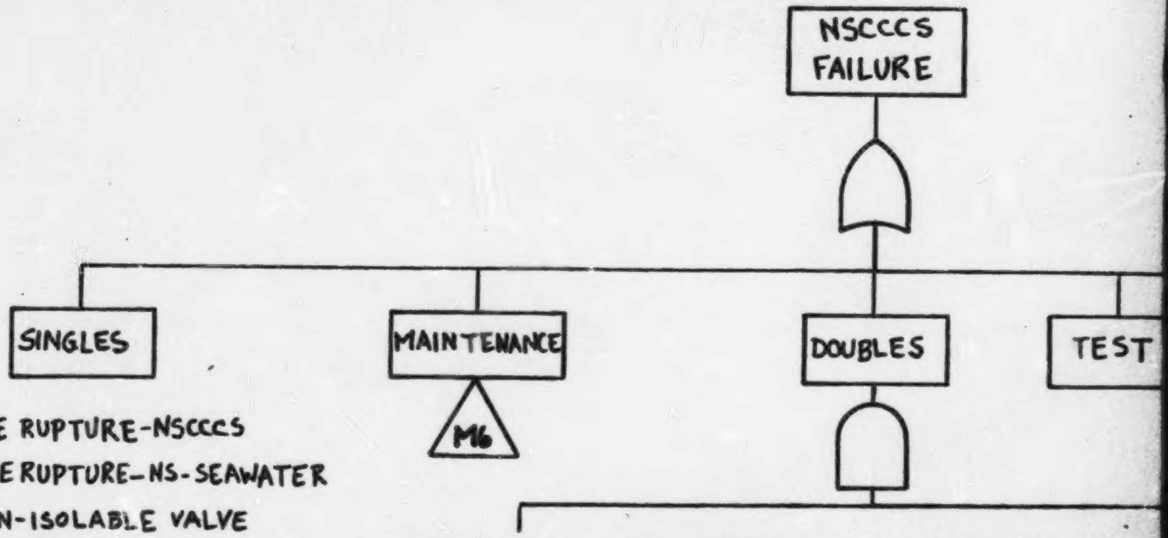

note 9
note 9
WP-2B
rain out
f
ervice
RWP-2A
train fails
1. RWP-2A fails to run
2. 4160 ES-3A fails
SWP-1A
train
out of
service
SWP-1B
train fails
ump B
RWP-2B
RWV-35
1. SWV-8
2. SWV-412
3. SWP-1A
1. SWP-1B fail to start
2. SWP-1B fail to run
3. 4160 ES-3B fail
4. ESAS train B fail (note 4)
5. SWV-9 fail to open
6. SWV-413 fail to open
7. SWV-6 closed
8. SWV-411 closed
9. SWV-3 closed
10. SWV-409 closed
11. SWV-140 closed
12. SWV-425 closed
13. SWV-164 closed
14. SWV-427 closed
NOTE 1

Figure E.5 (2/2) Simplified Fault Tree - NSCCCS; SWP-1C, RWP-2A Operating

[redacted]

BEST DOCUMENT AVAILABLE



1. PIPE RUPTURE-NSCCCS
2. PIPE RUPTURE-NS-SEAWATER
3. NON-ISOLABLE VALVE RUPTURE-FANS
4. NON-ISOLABLE VALVE RUPTURE-NSCCCS
5. NON-ISOLABLE VALVE RUPTURE-SEAWATER
6. NON-ISOLABLE EXPANSION JOINT RUPTURE-SEAWATER
7. EXPANSION TANK SWT-1, RUPTURE

1. RWP-2A FAIL TO START (note 10)
2. RWP-2A FAIL TO RUN
3. 4160 ES-3A FAIL
4. ESFAS-TRAIN A FAIL (note 4)
5. RWV-38-FAIL TO OPEN (note 2)
6. RWV-24-CLOSED } (note 1)
7. SWV-142-CLOSED } (note 1)
8. SWV-160-CLOSED (note 6)

---

1. SWP-1A FAIL TO RUN
2. 4160 ES-3A FAIL

---

1. SWHE-1B RUPTURE
2. SWHE-1C RUPTURE
3. SWHE-1D RUPTURE
4. SWHE-1B FAILURE
5. SWHE-1C FAILURE
6. SWHE-1D FAILURE

---

1. MISSILE DAMAGE TO CRDM COOLERS OR RCP MOTOR COOLERS

---

1. MISSILE DAMAGE TO PIPING OR FAN COOLERS IN CONTAINMENT

(note 12) 1. RWP-2B F
2. RWP-2B F
3. 4160 ES-3
(note 4) 4. ESFAS-T
(note 2) 5. RWV-35-
(note 1) 6. RWV-21-C
(note 1) 7. SWV-149-
(note 1) 8. SWV-168-

---

1. SWP-1B FA
2. 4160 ES-3

---

1. RWV-16 FA
2. RWV-8 FA
3. SWV-13 FA
4. SWV-17 FA
5. RWV-A FA
6. RWV-B FA
7. RWV-C FA
8. RWV-D FA
9. OPERATO HEAT EXC

---

1. FAILURE E
2. FAILURE O SWV-79, 80,

---

1. FAILURE O DETECT A

BEST DOCUMENT AVAILABLE

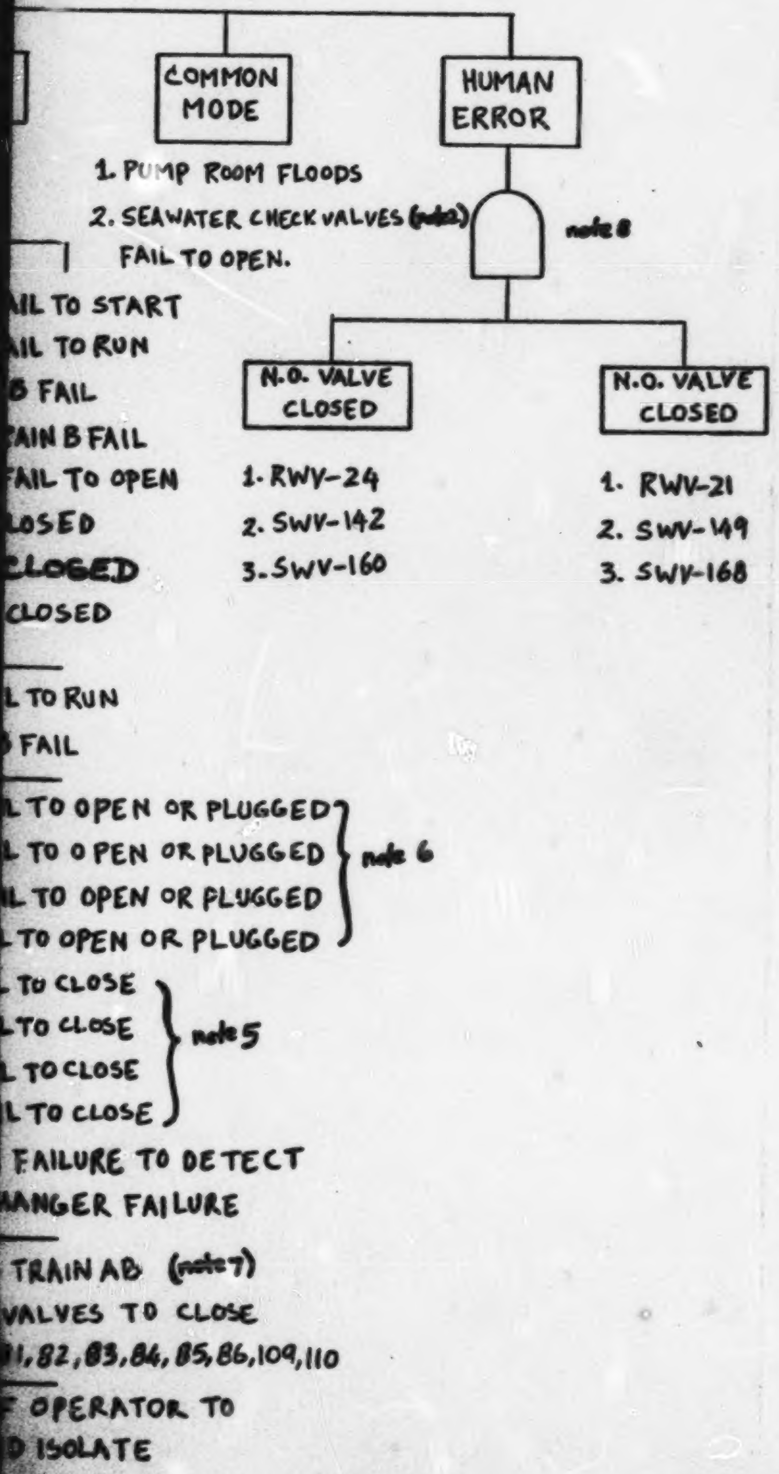
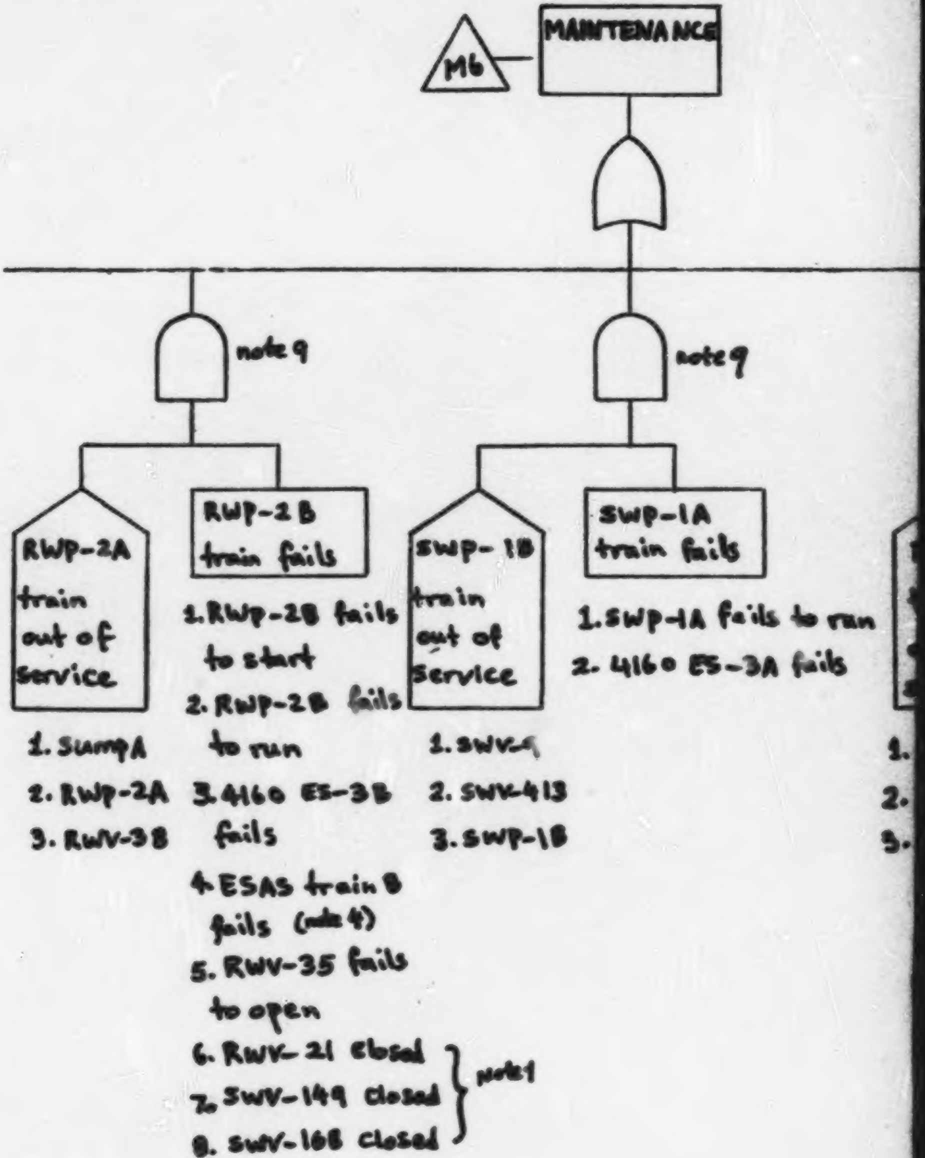

COMMON MODE
HUMAN ERROR
1. PUMP ROOM FLOODS
2. SEAWATER CHECK VALVES (note2) FAIL TO OPEN.
note 8
N.O. VALVE CLOSED
1. RWV-24
2. SWV-142
3. SWV-160
N.O. VALVE CLOSED
1. RWV-21
2. SWV-149
3. SWV-168
IL TO START
IL TO RUN
B FAIL
AIN B FAIL
FAIL TO OPEN
LOSED
CLOSED
CLOSED
L TO RUN
FAIL
L TO OPEN OR PLUGGED
L TO OPEN OR PLUGGED
IL TO OPEN OR PLUGGED
L TO OPEN OR PLUGGED
note 6
L TO CLOSE
L TO CLOSE
L TO CLOSE
IL TO CLOSE
note 5
FAILURE TO DETECT
ANGER FAILURE
TRAIN AB (note7)
VALVES TO CLOSE
1,82,83,84,85,86,109,110
OPERATOR TO
D ISOLATE

Figure E.6 (1/2) Simplified Fault Tree - NSCCCS; SWP-1A, RWP-1, Operating

BEST DOCUMENT AVAILABLE


M6
MAINTENANCE
note 9
note 9
RWP-2A train out of service
1. Sump A
2. RWP-2A
3. RWV-38
RWP-2B train fails
1. RWP-2B fails to start
2. RWP-2B fails to run
3. 4160 ES-3B fails
4. ESAS train B fails (note 4)
5. RWV-35 fails to open
6. RWV-21 closed
7. SWV-149 closed
8. SWV-168 closed
note 1
SWP-1B train out of service
1. SWV-9
2. SWV-413
3. SWP-1B
SWP-1A train fails
1. SWP-1A fails to run
2. 4160 ES-3A fails
1.
2.
3.

BEST DOCUMENT AVAILABLE

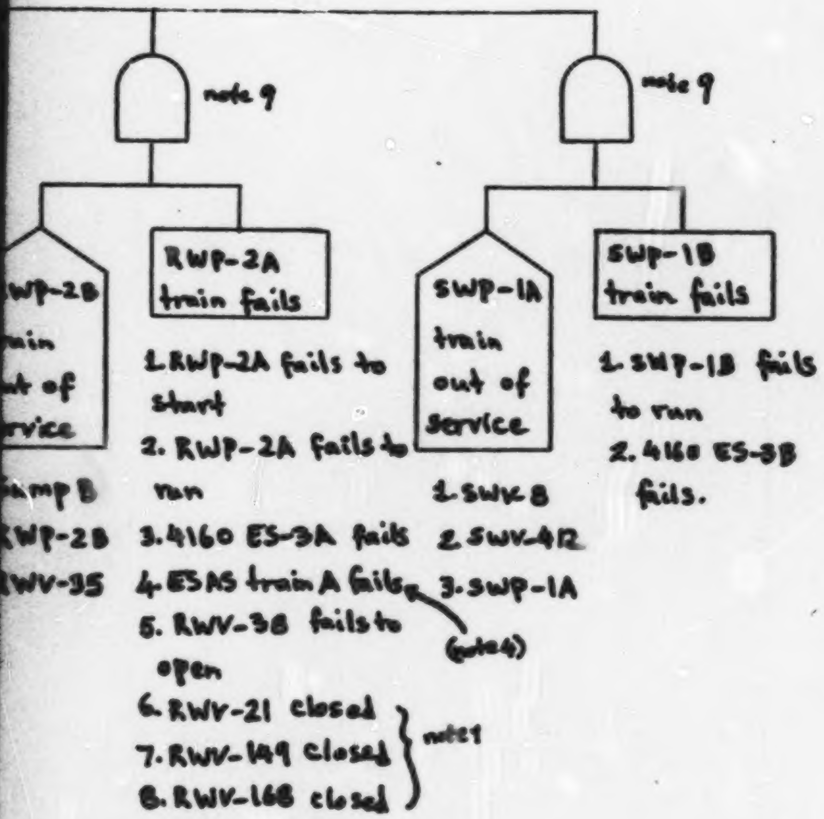

note 9
note 9
WP-2B
ain
t of
rvice
RWP-2A
train fails
SWP-1A
train
out of
Service
SWP-1B
train fails
amp B
WP-2B
WV-35
1. RWP-2A fails to start
2. RWP-2A fails to run
3. 4160 ES-3A fails
4. ESAS train A fails
5. RWV-38 fails to open
6. RWV-21 closed
7. RWV-149 closed
8. RWV-168 closed
note 1
(note 4)
1. SWV-8
2. SWV-412
3. SWP-1A
1. SWP-1B fails to run
2. 4160 ES-3B fails.

Figure E.6 (2/2) Simplified Fault Tree - NSCCCS; SWP-1A, RWP-1, Operating

[illegible]

Figures E.3 through E.6 Simplified Fault Trees

NOTES

1 These valves are normally open. These also appear in the Human Error contribution.

2 Both of these valves (RWV-38 and 35) are normally closed check valves in a seawater environment. Marine growth can be expected to occur on the valve during inoperative periods. This will alter the reliability over what can be expected in a freshwater environment. Each pump train is tested once a month on a staggered basis.

3 Four identical freshwater check valves, normally closed. Both valves in either pump train must open for success.

4 The capability is present to start the pumps manually. Low flow is alarmed in the control room. Pump speed is indicated in the control room.

5 The failed heat exchanger must be isolated. Inlet and outlet isolation valves must be closed. These are manual valves. Depending on which heat exchanger failed, the valve combinations are:

1B	1C	1D
SWV-18 RWV-6	SWV-19 RWV-15	SWV-20 RWV-16
SWV-14 RWV-14	SWV-15 RWV-7	SWV-16 RWV-8

Critical isolation time unknown.

6 Manual valves - locally operated.

7 Manual isolation is possible if detected. Critical isolation time unknown.

8 There are no single human errors. They all represent identical valves on redundant pumps.

9 Each of these conditions is allowed to exist for 72 hours. Components whose failure causes outage of a pump train are listed below the box.

10 Both of these pumps are inactive and located in non-flowing seawater. Each pump is tested once a month. Corrosion and marine growth on the pump internals may create high common mode coupling.

[redacted]

E.3 SYSTEM QUANTIFICATION

E.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The major contributor to the unavailability of the NSCCCS during the injection phase for cases where offsite power is available, is the failure of the NSSWS to remove heat from the NSCCCS. This is due to coupled hardware faults of the two seawater pumps (RWP-2A and -2B) or of the two check valves in the pump discharge (RWV-35 and -38). However, if offsite power is not available the dominant contributor to the system's unavailability is failure of both diesels to start and unavailability of power from fossil units CR-1 and -2. (The unavailability of both fossil units was assessed as 0.56).

The contribution of simultaneous hardware faults in both NSCCCS pump trains is about a factor of two smaller. These hardware faults include manual valves inadvertently left closed. Other contributors, about an order of magnitude smaller, are pump maintenance outages in one train and hardware failures in the other pump train.

The unavailability of the NSCCCS during the recirculation phase is dominated by faults that occurred during the injection phase in one train of either the NSCCCS or NSSWS and are not recovered for recirculation (they may not be recoverable faults) and faults that occur during the recirculation phase in the other train of NSCCCS or NSSWS. However, the NSCCCS unavailability during recirculation is about two orders of magnitude smaller than during injection.

E.3.2 SYSTEM FAULT TREE QUANTIFICATION — INJECTION PHASE

This section presents the quantification of the NSCCCS unavailability for required emergency operation of the NSCCCS during the injection phase of a postulated accident. The quantitative results are presented in table form with attached notes outlining the assumptions. To perform the fault tree quantification, the simplified fault tree representing the normally operating configuration (SWP-1C and RWP-1 in service, Figure E.3) was transformed into a modularized fault tree. Evaluating the system's unavailability for the normally operating configuration is conservative, since at least one emergency pump is required to start in each system (NSCCCS, NSSWS). For all other system operating configurations, at least one emergency pump is already running. Therefore, the relative high probability of failure to start of the emergency pump(s) does not contribute to the system's unavailability.

Table E.2 shows the NSCCCS success requirements, Table E.3 contains the top event definition for the modularized fault tree, and Figure E.7 shows the modularized fault tree for the NSCCCS. The unavailability of each gate is shown on the tree. Table E.4 shows the Boolean equation that represents the fault trees. Table E.5 shows the quantification of each gate by component and failure mode. The attached notes explain the assumptions used in the quantification. Table E.6 presents a summary of the point estimates for each gate and the error factors that were used in the sensitivity analysis.

Table E.2 NSCCCS Injection — System Success Requirements

INITIATOR	TRAINS	NOTES
B1, B2, B3, B4 Transient initiators	One pump flow for component cooling during injection.	1,2,3

NOTES: 1. The NSCCCS is required to supply containment cooling water to the containment cooling fans and high pressure system pumps MUP-1B and MUP-1A during injection and recirculation.

2. The NSCCCS is a single loop system but with dual pumps. The ultimate heat sink is the NSSWS, which is a dual loop system.

3. The NSSWS function of providing the ultimate heat sink for the NSCCCS is included in the analysis of the NSCCCS.

Table E.3 NSCCCS Injection — Top Event Definitions

BOOLEAN REPRESENTATION	TOP EVENT	NOTES
N	Failure of the NSCCCS to deliver one pump flow with ultimate heat removal for component cooling during injection	1
NC	Failure of the NSCCCS to deliver one pump flow during injection.	2
NR	Failure of the NSSWS to provide ultimate heat removal during injection.	3

NOTES: 1. The event N includes failures in both NSCCCS and in the NSSWS.

2. The event NC is defined for convenience of analysis.

3. The event NR is defined for convenience of analysis.

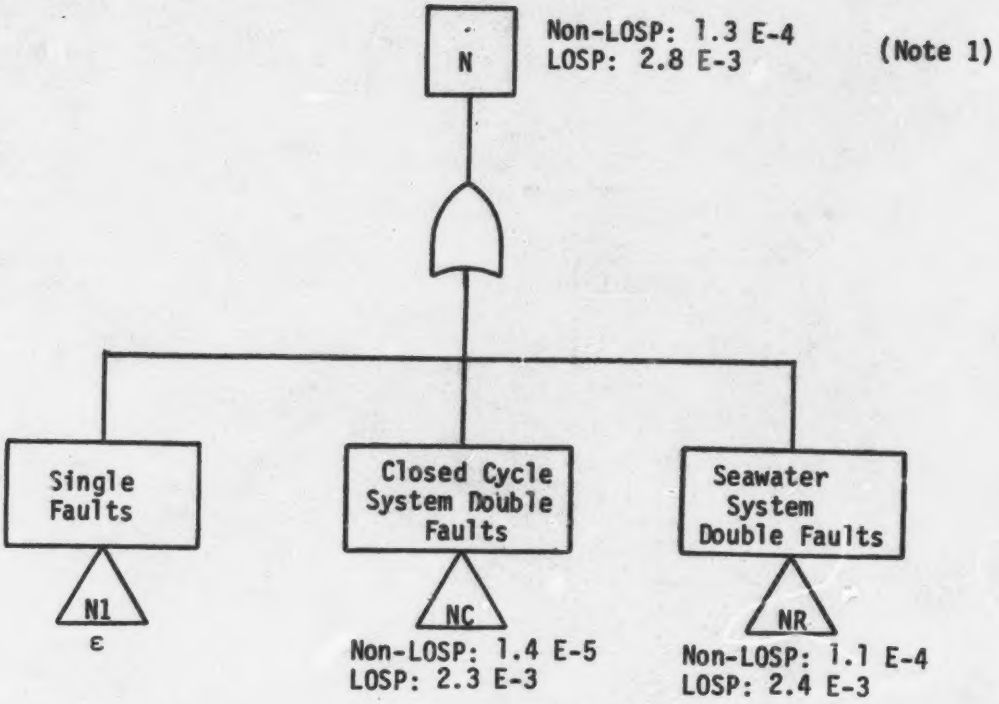

N
Non-LOSP: 1.3 E-4
LOSP: 2.8 E-3
(Note 1)
Single Faults
N1
ε
Closed Cycle System Double Faults
NC
Non-LOSP: 1.4 E-5
LOSP: 2.3 E-3
Seawater System Double Faults
NR
Non-LOSP: 1.1 E-4
LOSP: 2.4 E-3

Figure E.7 (1/3) Modularized Fault Tree For Event "N"

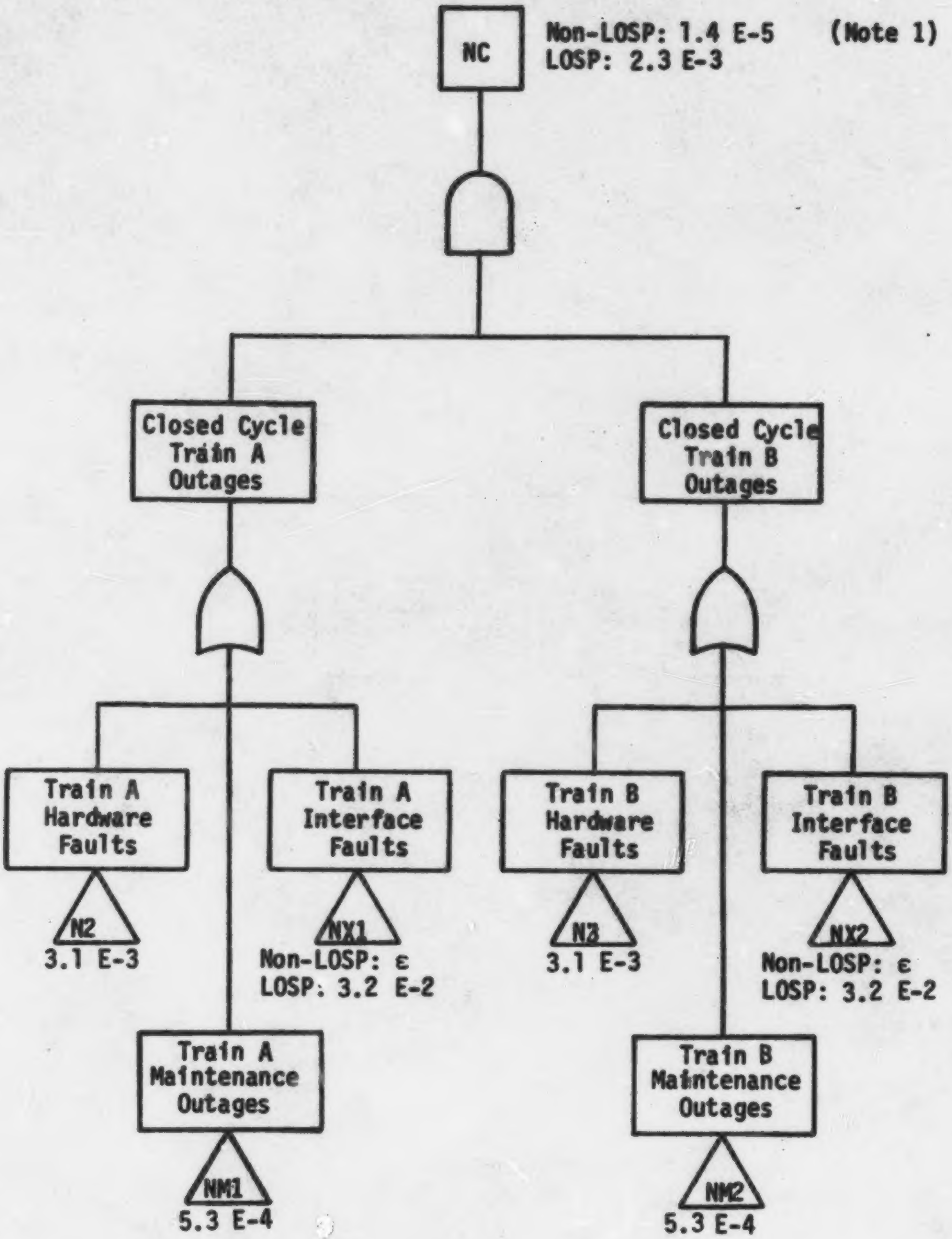

NC
Non-LOSP: 1.4 E-5 (Note 1)
LOSP: 2.3 E-3
Closed Cycle Train A Outages
Closed Cycle Train B Outages
Train A Hardware Faults
N2
3.1 E-3
Train A Interface Faults
NX1
Non-LOSP: ε
LOSP: 3.2 E-2
Train A Maintenance Outages
NM1
5.3 E-4
Train B Hardware Faults
N3
3.1 E-3
Train B Interface Faults
NX2
Non-LOSP: ε
LOSP: 3.2 E-2
Train B Maintenance Outages
NM2
5.3 E-4

Figure E.7 (2/3) Modularized Fault Tree For Event "NC"

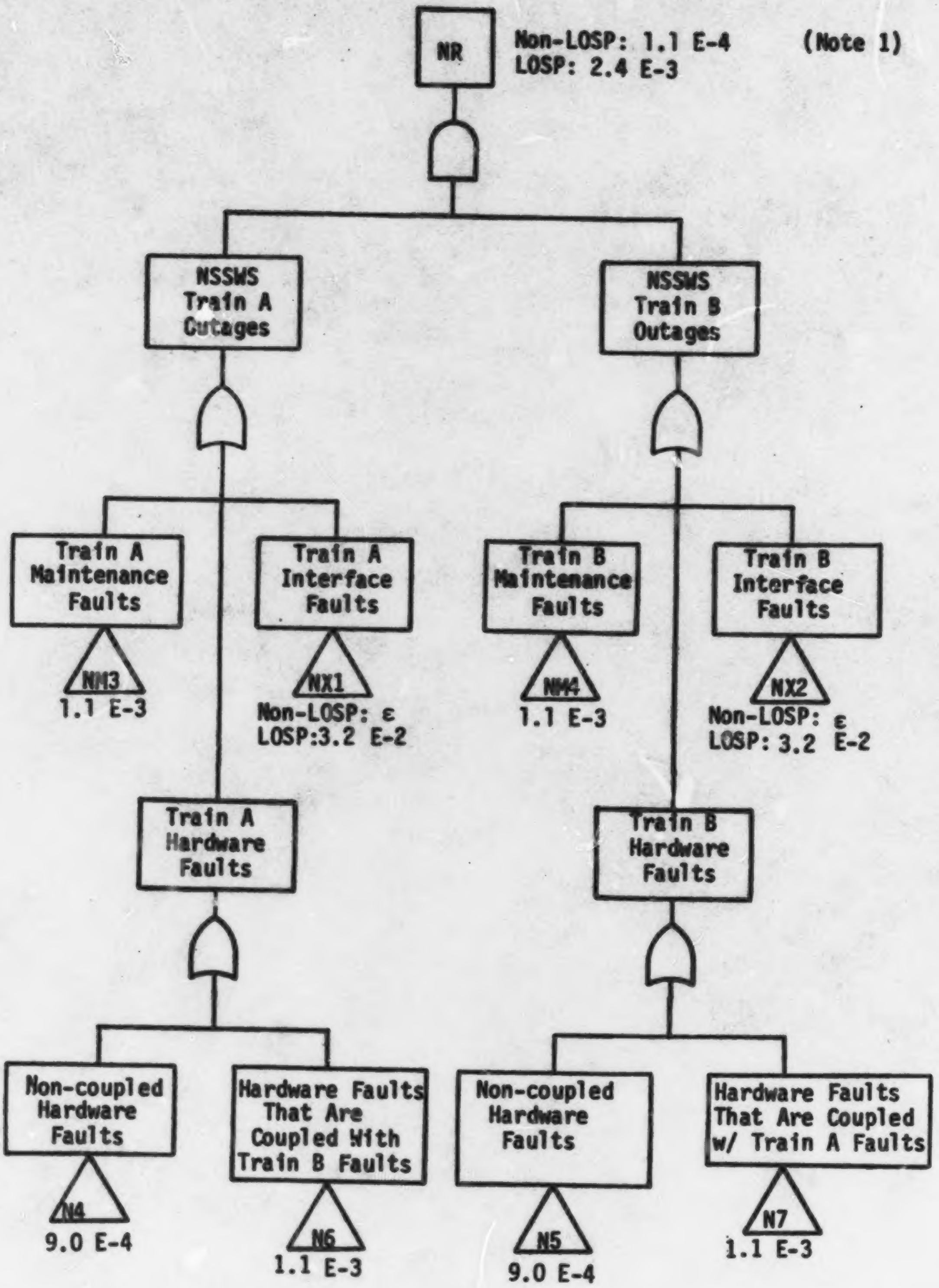

NR
Non-LOSP: 1.1 E-4
LOSP: 2.4 E-3
(Note 1)
NSSWS Train A Outages
NSSWS Train B Outages
Train A Maintenance Faults
NM3
1.1 E-3
Train A Interface Faults
NX1
Non-LOSP: ε
LOSP:3.2 E-2
Train B Maintenance Faults
NM4
1.1 E-3
Train B Interface Faults
NX2
Non-LOSP: ε
LOSP: 3.2 E-2
Train A Hardware Faults
Train B Hardware Faults
Non-coupled Hardware Faults
N4
9.0 E-4
Hardware Faults That Are Coupled With Train B Faults
N6
1.1 E-3
Non-coupled Hardware Faults
N5
9.0 E-4
Hardware Faults That Are Coupled w/ Train A Faults
N7
1.1 E-3

Figure E-7 (3/3) Modularized Fault Tree For Event "NR"

Figure E.7 NSCCCS - Injection

FAULT TREE

NOTES

1 These probabilities are based on Boolean reduced equations.

Table E.4 NSCCCS - Injection

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENT NOTES

$N = N1 + NC + NR$ 1

INTERMEDIATE EVENTS

$NC = (N2 + NM1 + NX1) \cdot (N3 + NM2 + NX2)$ 1

$NR = (N4 + N6 + NM3 + NX1) \cdot (N5 + N7 + NM4 + NX2)$ 1

$NX1 = ACA + DCA$ $NX2 = ACB + DCB$

BOOLEAN EQUATIONS REGROUPED FOR BOOLEAN REDUCTION

TOP EVENT

$$\begin{aligned} N = {} & N1 + ACA \cdot (N3 + N5 + N7 + NM2 + NM4) + \\ & + ACB \cdot (N2 + N4 + N6 + NM1 + NM3) + \\ & + ACA \cdot ACB + N2 \cdot (N3 + NM2) + N6 \cdot (N5 + NM4) + \\ & + N4 \cdot (N5 + N7 + NM4) + NM3 \cdot (N5 + N7) + \\ & + N6 \cdot N7 + N3 \cdot NM1 \end{aligned}$$ 2

Table E.4 NSCCCS Injection

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

NOTES:
1. These Boolean equations are not reduced to remove cross maintenance terms that are prohibited by Technical Specifications.
2. These Boolean equations have been reduced to remove cross maintenance terms that are prohibited by Technical Specifications. The DC - dependency is included in ACA and ACB.

Table E.5 (1/5) Event "N" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
N1		SINGLE FAILURES - VARIOUS PIPE AND VALVE RUPTURES			ε			1
N6·N7		COUPLED HARDWARE FAULTS			1.1 E-4	$2^+, 2^-$	B	5
	(RWP-2A) x (RWP-2B)	COUPLED SEAWATER PUMP FAILURE	(1.0 E-3)(.1)		1.0 E-4	$2^+, 2^-$	B	5
	(RWV-35) x (RWV-38)	COUPLED SEAWATER CHECKVALVE FAILURE	(1.0 E-4)(.1)		1.0 E-5	$2^+, 2^-$	B	5
					Σ=1.1 E-4			

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table E.5 (2/5) Event "NC" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR-1)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
N2		CLOSED CYCLE TRAIN A HARDWARE FAULTS			3.1 E-3	10^+, 10^-		
	PUMP SWP-1A	FAILS TO START	D		1.0 E-3	3^+, 3^-		
	PUMP SWP-1A	FAILS TO RUN	3.0 E-5	10	3.0 E-4	10^+, 10^-		2
	ESFAS-A	NO SIGNAL AND FAILURE TO RECOVER	(2.1 E-4)(0.1)		2.1 E-5			3, 6
	CHECK VALVE SWV-8	FAILS TO OPEN	D		1.0 E-4	3^+, 3^-		
	CHECK VALVE SWV-412	FAILS TO OPEN	D		1.0 E-4	3^+, 3^-		
	SWV-5	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
	SWV-410	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
	SWV-2	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
	SWV-408	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
	SWV-139	MANUAL VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
	SWV-424	MANUAL VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
	SWV-163	MANUAL VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
	SWV-426	MANUAL VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
					Σ=3.1 E-3			
NM1		MAINTENANCE OUTAGES			5.3 E-4			
	PUMP SWP-1A	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3^+, 3^-	M	
NX1		SYSTEM INTERFACE FAULTS						
ACA		AC TRAIN A FAILS						
		NON LOSP			ϵ			
		LOSP			3.2 E-2			
DCA		DC TRAIN A FAILS						
		NON LOSP			ϵ			
		LOSP			3.2 E-3			
N3		CLOSED CYCLE TRAIN B HARDWARE FAULTS			3.1 E-3	10^+, 10^-		
	PUMP SWP-1B	FAILS TO START	D		1.0 E-3	3^+, 3^-		
	PUMP SWP-1B	FAILS TO RUN	3.0 E-5	10	3.0 E-4	10^+, 10^-		2
	ESFAS-B	NO SIGNAL AND FAILURE TO RECOVER	(2.1 E-4)(0.1)		2.1 E-5			3,6
	CHECK VALVE SWV-9	FAILS TO OPEN	D		1.0 E-4	3^+, 3^-		
	CHECK VALVE SWV-413	FAILS TO OPEN	D		1.0 E-4	3^+, 3^-		
	SWV-6	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
	SWV-411	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
	SWV-3	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10^+, 10^-	H	4

BEST DOCUMENT AVAILABLE

Table E.5 (3/5) Event "NC" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
	SWV-409	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02X1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
	SWV-140	MANUAL VALVES INADVERTENTLY CLOSED	(.02X1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
	SWV-425	MANUAL VALVES INADVERTENTLY CLOSED	(.02X1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
	SWV-164	MANUAL VALVES INADVERTENTLY CLOSED	(.02X1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
	SWV-427	MANUAL VALVES INADVERTENTLY CLOSED	(.02X1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
					Σ=3.1 E-3			
MM2		MAINTENANCE OUTAGES			5.3 E-4	3^+, 3^-	M	
	PUMP SWP-1B	OUT FOR MAINTENANCE	02/720	19	5.3 E-4	3^+, 3^-	M	
MX2		SYSTEM INTERFACE FAULTS						
ACB		AC TRAIN B FAILS						
		NON LOSP			ϵ			
		LOSP			5.2 E-2			
DCB		DC TRAIN B FAILS						
		NON LOSP			ϵ			
		LOSP			3.2 E-3			

BEST DOCUMENT AVAILABLE

Table E.5 (4/5) Event "NR" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
N4		NON-COUPLED TRAIN A HARDWARE FAULTS			9.0 E-4	10^+, 10^-	H	
	PUMP RWP-2A	FAILS TO RUN	3.0 E-5	10	3.0 E-4	10^+, 10^-		2
	ESFAS-A	NO SIGNAL AND FAILURE TO RECOVER	(2.1E-4)(0.1)		2.1 E-5			3, 6
	RWV-24	BUTTERFLY VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
	SWV-142	MANUAL VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
	SWV-166	MANUAL VALVE INADVERTENTLY CLOSED	(.02)(1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
					Σ=9.0 E-4			
N6		COUPLED TRAIN A HARDWARE FAULTS			1.1 E-3	3^+, 3^-	S	
	PUMP RWP-2A	FAILS TO START	D		1.0 E-3	3^+, 3^-	S	
	CHECK VALVE RWV-38	FAILS TO OPEN	D		1.0 E-4	3^+, 3^-	S	
					Σ=1.1 E-3			
NM3		TRAIN A MAINTENANCE OUTAGES			1.1. E-3	3^+, 3^-		
	PUMP RWP-2A	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3^+, 3^-	M	
	CHECK VALVE RWV-38	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3^+, 3^-	M	
					Σ=1.1 E-3			

Table E.5 (5/5) Event "NR" Quantification (Continued)

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
N5		NON COUPLED HARDWARE FAULTS IN TRAIN B			9.0 E-4	10^+, 10^-	H	
	PUMP RWP-2B	FAILS TO RUN	3.0 E-5	10	3.0 E-4	10^+, 10^-		2
	ESFAS-B	NO SIGNAL AND OPERATOR FAILS TO RECOVER	2.1 E-4(0.1)		2.1 E-5			3,6
	RWV-21	BUTTERFLY VALVE INADVERTENTLY LEFT CLOSED	(.02)(1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
	SWV-149	MANUAL VALVE INADVERTENTLY LEFT CLOSED	(.02)(1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
	SWV-168	MANUAL VALVE INADVERTENTLY LEFT CLOSED	(.02)(1.0 E-2)		2.0 E-4	10^+, 10^-	H	4
					Σ=9.0 E-4			
N7		COUPLED TRAIN B HARDWARE FAULTS			1.1 E-3	3^+, 3^-	S	
	PUMP RWP-2B	FAILS TO START	D		1.0 E-3	3^+, 3^-	S	
	CHECK VALVE RWV-35	FAILS TO OPEN	D		1.0 E-4	3^+, 3^-	S	
					Σ=1.1 E-3			
N14		TRAIN B MAINTENANCE OUTAGES			1.1. E-3	3^+, 3^-	M	
	PUMP RWP-2B	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3^+, 3^-	M	
	CHECK VALVE RWV-35	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	3^+, 3^-	M	
					Σ=1.1 E-3			

BEST DOCUMENT AVAILABLE

Table E.5 NSCCCS - Injection

QUANTIFICATION TABLES

NOTES

1 The NSCCCS is a normally operating system. It was assumed that pipe or valve ruptures would be detected when they occur, and repaired. Therefore, these faults were assessed to be negligibly small.

2 The time duration for injection can vary from 0.5 hrs. to 10 hrs., depending on the LOCA size. A fault duration time of 10 hrs. was conservatively chosen for the analysis.

3 The failure of ESFAS to actuate single equipment was assessed as 2.1 E-4 (Event ISS1 in ESAS quantification). Although this number is insignificant, it is correct only for the B4 LOCA. It is conservative for the other LOCA cases. Failure to recover was assumed to be 0.1 per act.

4 The frequency of maintenance was assumed to be 0.02 acts per month. The probability of leaving a valve in the incorrect position after maintenance was assessed as 1E-2 per maintenance act.

5 The failure of these components was assumed coupled since they see the same seawater environment. A coupling coefficient (β factor) of 0.1 was assumed.

6 Failure of ESAS to provide actuation signals to both trains is not included because the potential for recovery is high enough to make this contribution negligible.

Table E.6 NSCCCS - Injection Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
N1	ε
N2	3.1 E-3
NM1	5.3 E-4
N3	3.1 E-3
NM2	5.3 E-4
N4	9.0 E-4
N6	1.1 E-3
NM3	1.1 E-3
N5	9.0 E-4
N7	1.1 E-3
NM4	1.1 E-3
N6·N7	1.1 E-4
ACA	ε* 3.2 E-2**
ACB	ε* 3.2 E-2**
ACA·ACB	2.3 E-3

*offsite power available
**offsite power not available

E.3.3 SYSTEM FAULT TREE QUANTIFICATION — RECIRCULATION PHASE

This section presents the quantification of the NSCCCS unavailability for required emergency operation during the recirculation phase of a postulated accident. As for the injection phase, modularized fault trees were constructed. Credit was given for recovery of certain failures which occurred during the injection phase, e.g., events N*3 and N*4 in the quantification tables.

Table E.7 shows the NSCCCS success requirements. Table E.8 contains the top event definitions, and Figure E.8 shows the modularized fault tree. The unavailability of each gate is shown on these trees, as well as the top event unavailabilities. Table E.9 shows the Boolean equations that represent the fault tree. Table E.10 shows the quantification of each gate, by component and failure mode. The attached notes explain the assumptions used in the quantification. Table E.11 presents a summary of the point estimates for each gate and the error factors that were used in the sensitivity analysis.

Table E.7 NSCCCS Recirculation — System Success Requirements

INITIATOR	TRAINS	NOTES
B1, B2, B3, B4 transient initiators	One pump flow for component cooling during recirculation	1,2,3

NOTES: 1. The NSCCCS is required to supply containment cooling water to the containment cooling fans and high pressure system pumps MUP-1B and MUP-1A during injection and recirculation.

2. The NSCCCS is a single loop system but with dual pumps. The ultimate heat sink is the raw water system, which is a dual loop system.

3. The NSSWS function of providing the ultimate heat sink for the NSCCCS is included in the analysis of the NSCCCS.

Table E-8 NSCCCS Recirculation — Top Event Definitions

BOOLEAN REPRESENTATION	TOP EVENT	NOTES
N*	Failure of the NSCCCS to deliver one pump flow with ultimate heat removal for cooling during recirculation.	1
NC1*(NC2*)	Failure of the NSCCCS Train A(B) to deliver pump flow during recirculation.	2
NR1* (NR2*)	Failure of the NSSWS Train A(B) to deliver pump flow during recirculation.	3

NOTES: 1. The event N* includes failures in both the closed cycle portion of the cooling system and in the seawater portion of the system.

2. The event NC1* (NC2*) is defined for convenience of analysis.

3. The event NR1*(NR2*) is defined for convenience of analysis.

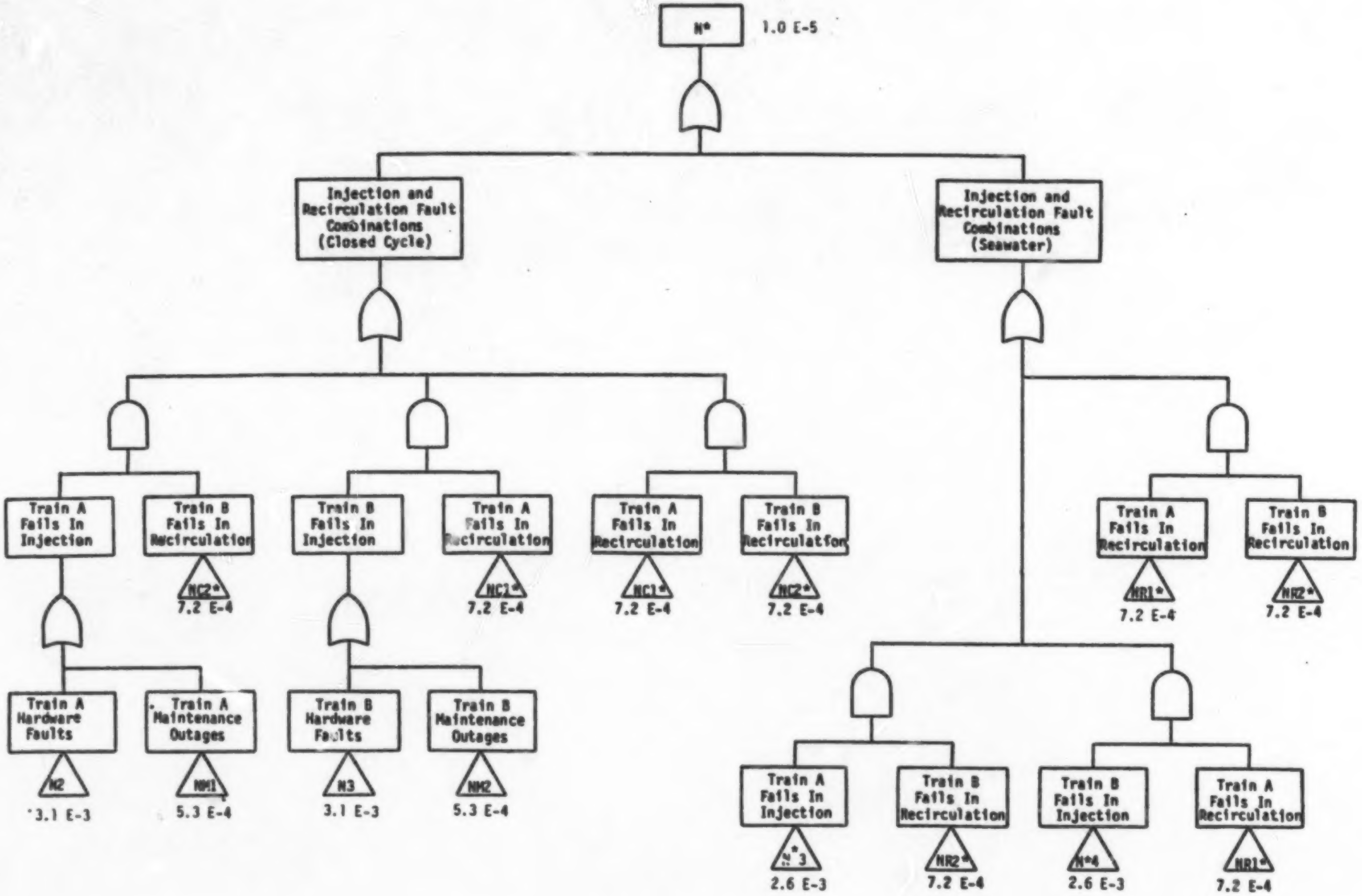

N*
1.0 E-5
Injection and Recirculation Fault Combinations (Closed Cycle)
Injection and Recirculation Fault Combinations (Seawater)
Train A Fails In Injection
Train B Fails In Recirculation
NC2*
7.2 E-4
Train B Fails In Injection
Train A Fails In Recirculation
NC1*
7.2 E-4
Train A Fails In Recirculation
NC1*
7.2 E-4
Train B Fails In Recirculation
NC2*
7.2 E-4
Train A Fails In Recirculation
NR1*
7.2 E-4
Train B Fails In Recirculation
NR2*
7.2 E-4
Train A Hardware Faults
N2
3.1 E-3
Train A Maintenance Outages
NM1
5.3 E-4
Train B Hardware Faults
N3
3.1 E-3
Train B Maintenance Outages
NM2
5.3 E-4
Train A Fails In Injection
N*3
2.6 E-3
Train B Fails In Recirculation
NR2*
7.2 E-4
Train B Fails In Injection
N*4
2.6 E-3
Train A Fails In Recirculation
NR1*
7.2 E-4

Figure E.8 (1/3) Modularized Fault Tree For Event "N*"

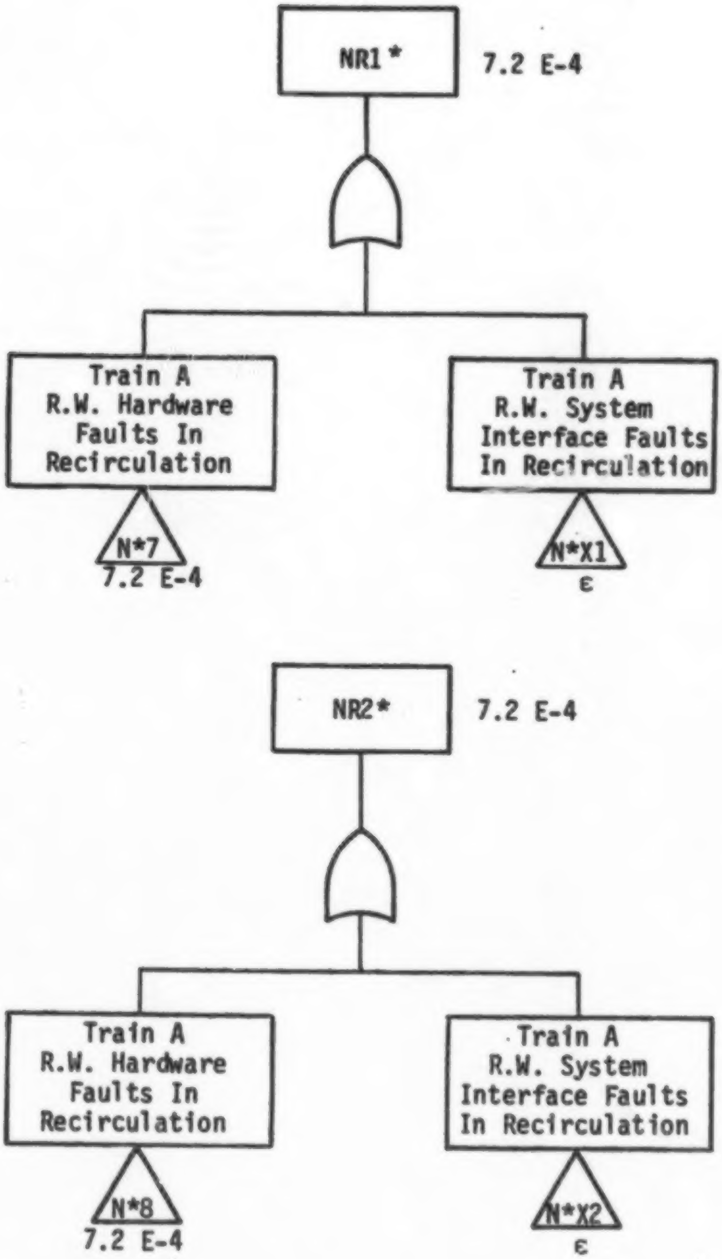

NR1*
7.2 E-4
Train A R.W. Hardware Faults In Recirculation
Train A R.W. System Interface Faults In Recirculation
N*7
7.2 E-4
N*X1
ε
NR2*
7.2 E-4
Train A R.W. Hardware Faults In Recirculation
Train A R.W. System Interface Faults In Recirculation
N*8
7.2 E-4
N*X2
ε

Figure E.8 (2/3) Modularized Fault Tree For Event "NR1*" and "NR2*"

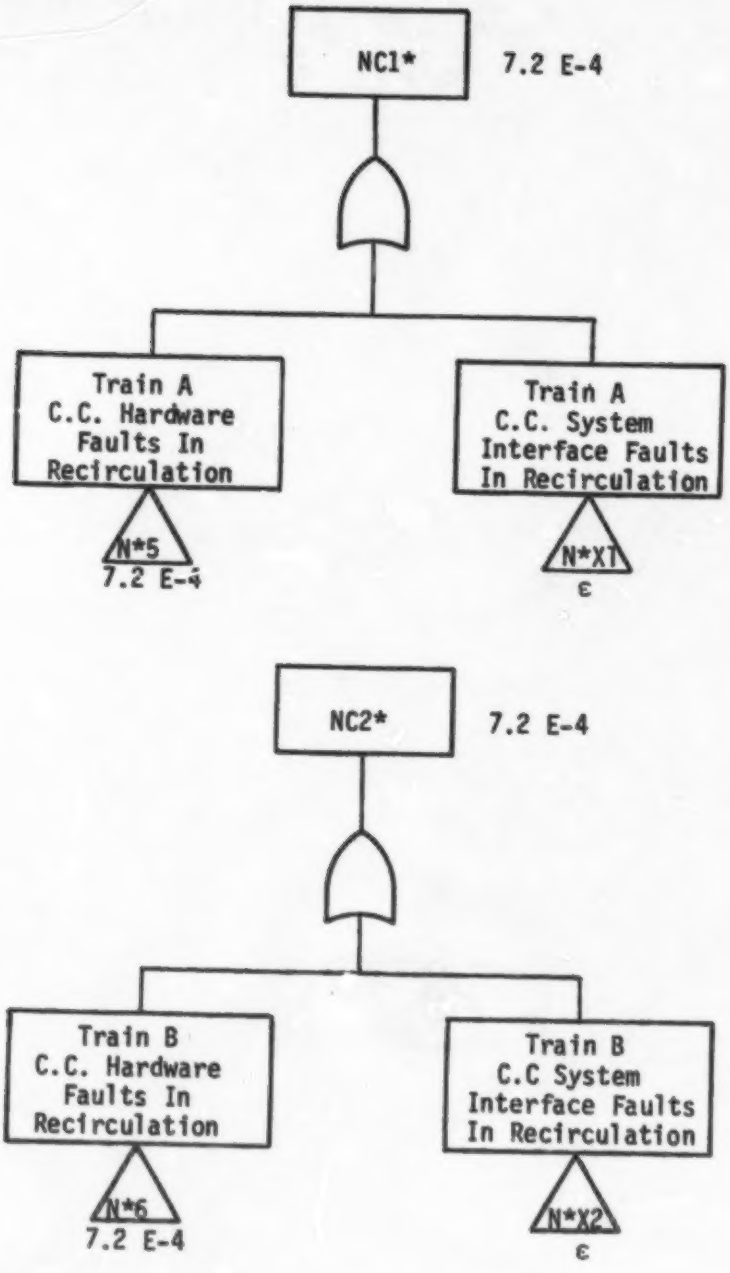

NC1*
7.2 E-4
Train A C.C. Hardware Faults In Recirculation
N*5
7.2 E-4
Train A C.C. System Interface Faults In Recirculation
N*X1
ε
NC2*
7.2 E-4
Train B C.C. Hardware Faults In Recirculation
N*6
7.2 E-4
Train B C.C System Interface Faults In Recirculation
N*X2
ε

Figure E.8 (3/3) Modularized Fault Tree For Event "NC1*" and "NC2*"

Table E.9 NSCCCS - Recirculation

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENT NOTES

$$\begin{aligned} N* &= NC1*\cdot(N3+NM2) + NC2*\cdot(N2+NM1) + NC1*\cdot NC2* + \\ &\quad + NR1*\cdot N*4 + NR2*\cdot N*3 + NR1*\cdot NR2* \qquad 1 \end{aligned}$$

$$NC1* = N*5 + N*X1$$

$$NC2* = N*6 + N*X2$$

$$NR1* = N*7 + N*X1$$

$$NR2* = N*8 + N*X2$$

INTERMEDIATE EVENTS

$$N*X1 = ACA*$$

$$N*X2 = ACB*$$

BOOLEAN EQUATIONS REGROUPED FOR BOOLEAN REDUCTION

TOP EVENT

$$\begin{aligned} N* &= N*5\cdot N*6 + N*8 + N*4\cdot N*7 + N*7\cdot N*8 + \\ &\quad + ACA*\cdot ACB* + ACA*\cdot(N3+NM2+N*6+N*4+N*8) + \\ &\quad + ACB*\cdot(N2+NM1+N*5+N*3+N*7) + \\ &\quad + N*5\cdot(N3+NM2) + N*6\cdot(N2+NM1) \qquad 2 \end{aligned}$$

NOTES: 1. This equation has not been reduced.

2. This equation is Boolean reduced.

Table E.10 (1/5) Event "N*3" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
N*3		RAW WATER TRAIN A FAILS IN INJECTION AND IS NOT RECOVERED			2.6 E-3	3+, 3-	S	
	PUMP RWP-2A	FAILS TO RUN	3.0 E-5	10	3.0 E-4	10^+, 10^-		
	ESFAS-A	NO SIGNAL AND FAILURE TO RECOVER	(2.1 E-4)(0.1)		2.1 E-5			
	RWV-24	VALVE CLOSED AND FAILURE TO RECOVER	(2.0 E-4)(.1)		2.0 E-5	10^+, 10^-	H	1
	SWV-142	VALVE CLOSED AND FAILURE TO RECOVER	(2.0 E-4)(.1)		2.0 E-5	10^+, 10^-	H	1
	SWV-166	VALVE CLOSED AND FAILURE TO RECOVER	(2.0 E-4)(.1)		2.0 E-5	10^+, 10^-	H	1
N6		SEE NSCCCS INJECTION QUANTIFICATION TABLES			1.1 E-3	3^+, 3^-	S	
NM3		SEE NSCCCS INJECTION QUANTIFICATION TABLES			1.1 E-3	3^+, 3^-	M	
					Σ=2.6 E-3	3^+, 3^-		

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table E.10 (2/5) Event "N*4" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
N*4		RAW WATER TRAIN B FAILS IN INJECTION AND IS NOT RECOVERED			2.6 E-3	3^+, 3^-	S	
	PUMP RWP-2B	FAILS TO RUN	3.0 E-5	10	3.0 E-4	10^+, 10^-		
	ESFAS-B	NO SIGNAL AND OPERATOR FAILS TO RECOVER	(2.1 E-4)(0.1)		2.1 E-5			
	RWV-21	BUTTERFLY VALVE INADVERTENTLY LEFT CLOSED AND FAILURE TO RECOVER	(2.0 E-4)(0.1)		2.0 E-5	10^+, 10^-	H	1
	SWV-149	MANUAL VALVE INADVERTENTLY LEFT CLOSED AND FAILURE TO RECOVER	(2.0 E-4)(0.1)		2.0 E-5	10^+, 10^-	H	1
	SWV-168	MANUAL VALVE INADVERTENTLY LEFT CLOSED AND FAILURE TO RECOVER	(2.0 E-4)(0.1)		2.0 E-5	10^+, 10^-	H	1
N7		SEE NSCCCS INJECTION QUANTIFICATION TABLES			1.1 E-3	3^+, 3^-	S	
NM4		SEE NSCCCS INJECTION QUANTIFICATION TABLES			1.1 E-3	3^+, 3^-	M	
					Σ=2.6 E-3	3^+, 3^-		

Table E.10 (3/5) Events "N2, N3, NM1, NM2" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR-1)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
N2		CLOSED CYCLE NSCCCS TRAIN A INJECTION FAULTS - SEE NSCCCS INJECTION QUANTIFICATION TABLES			3.2 E-3	10^+, 10^-	H	
NM1		SEE NSCCCS INJECTION QUANTIFICATION TABLES			5.3 E-4	3^+, 3^-	M	
N3		CLOSED CYCLE NSCCCS TRAIN B INJECTION FAULTS - SEE NSCCCS INJECTION QUANTIFICATION TABLES			3.2 E-3	10^+, 10^-	H	
NM2		SEE NSCCCS INJECTION QUANTIFICATION TABLES			5.3 E-4	3^+, 3^-	M	

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table E.10 (4/5) Events "NC1*, NC2*" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
N*5		CLOSED CYCLE TRAIN A HARDWARE FAULTS DURING RECIRCULATION			7.2 E-4			
	PUMP SWP-1A	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10^+, 10^-		
N*X1		CLOSED CYCLE TRAIN A SYSTEM INTERFACE FAULTS DURING RECIRCULATION			ε			
ACA*		AC TRAIN A						
		FAILS DURING RECIRCULATION			ε			
N*6		CLOSED CYCLE TRAIN B HARDWARE FAULTS DURING RECIRCULATION			7.2 E-4			
	PUMP SWP-1B	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10^+, 10^-		
N*X2		CLOSED CYCLE TRAIN B SYSTEM INTERFACE FAULTS DURING RECIRCULATION			ε			
ACB*		AC TRAIN B						
		FAILS DURING RECIRCULATION			ε			

Table E.10 (5/5) Events "NR1*, NR2*" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
N*7		RAW WATER TRAIN A HARDWARE FAULTS DURING RECIRCULATION			7.2 E-4			
	PUMP RWP-2A	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10^+, 10^-		
N*X1		SEE NC1*, NC2*, QUANTIFICATION TABLES			ε			
N*8		RAW WATER TRAIN B HARDWARE FAULTS DURING RECIRCULATION			7.2 E-4			
	PUMP RWP-2B	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10^+, 10^-		
N*X2		SEE NC1*, NC2* QUANTIFICATION TABLES			ε			

BEST DOCUMENT AVAILABLE

Table E.10 NSCCCS - Recirculation

QUANTIFICATION TABLES

NOTES

1 Valves inadvertently closed and fail to recover were assessed as 2.0 E-4 probability of the valve being in the closed position times 0.1 probability of no recovery. See NSCCCS - Injection Quantification Tables.

Table E.11 NSCCCS - Recirculation Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
N*5	7.2 E-4
N*X1	ε
ACA*	ε
N*6	7.2 E-4
N*X2	ε
ACB*	ε
N*7	7.2 E-4
N*8	7.2 E-4
N*3	2.6 E-3
N*4	2.6 E-3

APPENDIX F

DECAY HEAT CLOSED CYCLE COOLING SYSTEM (DHCCCS)

APPENDIX F DECAY HEAT CLOSED CYCLE COOLING SYSTEM (DHCCCS)

F.1 SYSTEM DESCRIPTION AND OPERATION

The purpose of the Decay Heat Closed Cycle Cooling System (DHCCCS) is (1) to remove decay heat from the Low Pressure Heat Removal System and (2) to provide component cooling for bearings and motors in the Low Pressure Heat Removal System, the Containment Spray System, and one train of the High Pressure Injection System. In addition, the DHCCCS provides component cooling for components that are part of the raw seawater (or ultimate heat sink) portion (DHSS) of the DHCCCS. The DHCCCS is required to operate for decay heat removal and component cooling for all accidents or transients that require the Low Pressure Heat Removal System, the Containment Spray System, or the High Pressure Injection System (makeup pump MUP-1C only). Operation may be required during both the injection and recirculation phases of the accident sequence. Operation is also required during normal operation to remove reactor decay heat during shutdown.

F.1.1 SYSTEM DESCRIPTION

The DHCCCS consists of two loops, a closed cycle loop that removes decay heat and component heat, and a once-through system (the raw water, or seawater system) that removes heat from the closed cycle loop and discharges it to the seawater discharge canal. Both the once-through seawater system, and the closed cycle system are doubly redundant, consisting of Trains A and B. Train A of the seawater system removes heat from Train A of the closed cycle system, and Train B of the seawater system removes heat from Train B of the closed cycle system. The trains are independent of each other and each is rated at 100% capacity for decay heat removal and cooling of components they serve. Figures F.1 and F.2 show simplified one-line diagrams of the closed cycle and seawater portions of the DHCCCS, respectively.

The design flow rate in each of the closed cycle trains is 3200 gpm, 3000 of which goes through the respective DHRS heat exchanger. The remaining 200 gpm is used for pump cooling. Maximum heat rejection capability per loop, under emergency conditions, is 120x10^6 BTU/hr. Under these conditions, the hot leg operates at 140°F and the cold leg at 105°F. The pump develops an 80 foot head. Each loop has its own surge tank which is pressurized to 5-10 psig. This is not necessary for NPSH requirements. Both the source and sink heat exchangers are shell and tube, with the closed cycle water on the shell side of both.

There are no MOV's or automatic valves in the closed cycle portion of the system. Each loop has manual blocking valves for the major components. These are not locked and are locally indicated. The only locked valves in the system are those in the cooling lines to the motors. The pumps in the closed cycle portion of the system are forced air cooled. A fan cooler assembly (AHF-15A or 15B) in each train provides motor cooling. AHF-15A and 15B are cooled by their respective DHCCCS loops. Both the pumps and AHF-15 are powered by the 480V ESMCC's. The pump bearing is self cooled.

The major lines in the closed cycle portion of the system are 12 inch pipes. These supply flow to the heat exchangers. The majority of the flow is directed to the low pressure heat removal heat exchanger. The motor cooling loads are through smaller 2-3 inch lines directed from the main pipe. The flow to the low pressure system heat exchanger is controlled by a two-valve bypass. The flow can be totally shunted from the heat exchanger. The two valves are controlled together by a single circuit. These are regulated to control the cooldown rate after a normal shutdown. During emergency operation, the total flow is directed through the heat exchanger. The position of these valves before ESAS is such that total flow is directed through the heat exchanger.

The seawater portion of the system (DHSS) transports heat from the closed cycle portion to the seawater discharge canal. Each seawater train services its respective closed cycle train. The seawater system is a once-through, open cooling system. Seawater flows by gravity from the intake canal to the seawater sump through 48 inch pipes. The two pumps from the respective seawater trains are installed in separate compartments in the seawater sump to allow the isolation of either compartment for service without disabling both trains.

Each seawater pump takes suction from the seawater sump, pumps water through its respective heat exchanger and into the discharge canal. There are no other cooling loads on the system. The pump motors are cooled by the respective freshwater (closed cycle) cooling train. They are powered by the 4160V ES buses. The bearing is cooled by domestic water supply. If that fails, the demineralized water supply will back-up the domestic water. If both those fail, the seawater will back into the bearing. This provides adequate cooling although it is not desirable for long term cooling because of corrosion considerations.

Each 300 HP RW pump supplies 9700 gpm at a 75 foot head. Pump discharge piping is 20 inches, but it diffuses to 24 inches before it reaches the heat exchanger. The temperature rise through the heat exchanger is only 6°F. Technical Specifications (T.S.3.4.7.5) prohibit plant power operation if the inlet temperature rises above 105°F.

The seawater trains have no MOV's or remotely operated valves. Each pump has a 20 inch check valve in the discharge. There are no locked valves in the system. Manual valves are locally indicated. Table F.1, reproduced from the Crystal River FSAR, contains design information on specific DHCCCS equipment.

F.1.2 DHCCCS SYSTEM OPERATION

The DHCCCS is required to operate when any of the components it serves are in operation. These consist of pumps in the Low Pressure Heat Removal System, Containment Spray System, and High Pressure Injection System pump MUP-1C. The DHCCCS is required during emergency operation for component cooling and decay heat removal, and during normal operation for decay heat removal on reactor shutdown. Operation of the system is initiated either manually, or on the 1500 psi ESAS trip signal.

Normal Operation - This system has no function when the plant is at power. Under normal shutdown, the system removes decay heat from heat exchangers DHHE-1A/1B. The system is normally in a standby state with its valves aligned for emergency service.

Emergency Operation - This system is activated on ES signal. Activation consists of starting RWP-3A/3B and DCP-1A/1B.

Control - Pumps can be manually started or stopped from the control room or locally at the breakers. Valves DCV-18/DCV-178 are manually controlled from the control room (PSA panel).

Testing of the closed cycle pumps does not require reconfiguration of the loop. Testing of each pump is done once a month per SP-340. DCV-18/17 and DCV-178/177 are stroked once a quarter. All valves are checked for proper position once a month per SP-347. Testing of the two loops is alternated on a two-week staggered basis.

Each raw water pump is also tested once a month per SP-340. Check valves RWV-34 and 37 are checked with the pumps. Valves are checked for proper position once a month per SP-347. Testing is on a two-week staggered basis. Maintenance was assumed to be performed only on major components such as pumps and valves.

Table F.1

Component Design Information

Decay Heat Closed Cycle Heat Exchangers

Number	2
Type	Shell and Tube
Duty Btu/h	120×10^6 Normal
Sea Cooling Water Flow (tubeside), gpm	9700
Sea Cooling Water Temperature, F	85
Closed Cycle Cooling Water Outlet Temp, F	105 Max
Closed Cycle Cooling Water Flow (shell side), gpm	3200
Design Pressure, Shell/Tube, psig	100/75
Max Design Temperature, Shell/Tube, F	200/140
Tube Material	90/10 Cu-Ni
Shell Material	Carbon Steel, ASTM
Channel Material	2% Nickel Cast Iron
Code/Seismic Class	ASME Section VIII/I

Decay Heat Closed Cycle Cooling Water Pumps

Number	2
Flow, gpm	3200
Design Head, ft	80
Design Pressure, psig	100
Max Design Temperature, F	135
Seismic Class	I

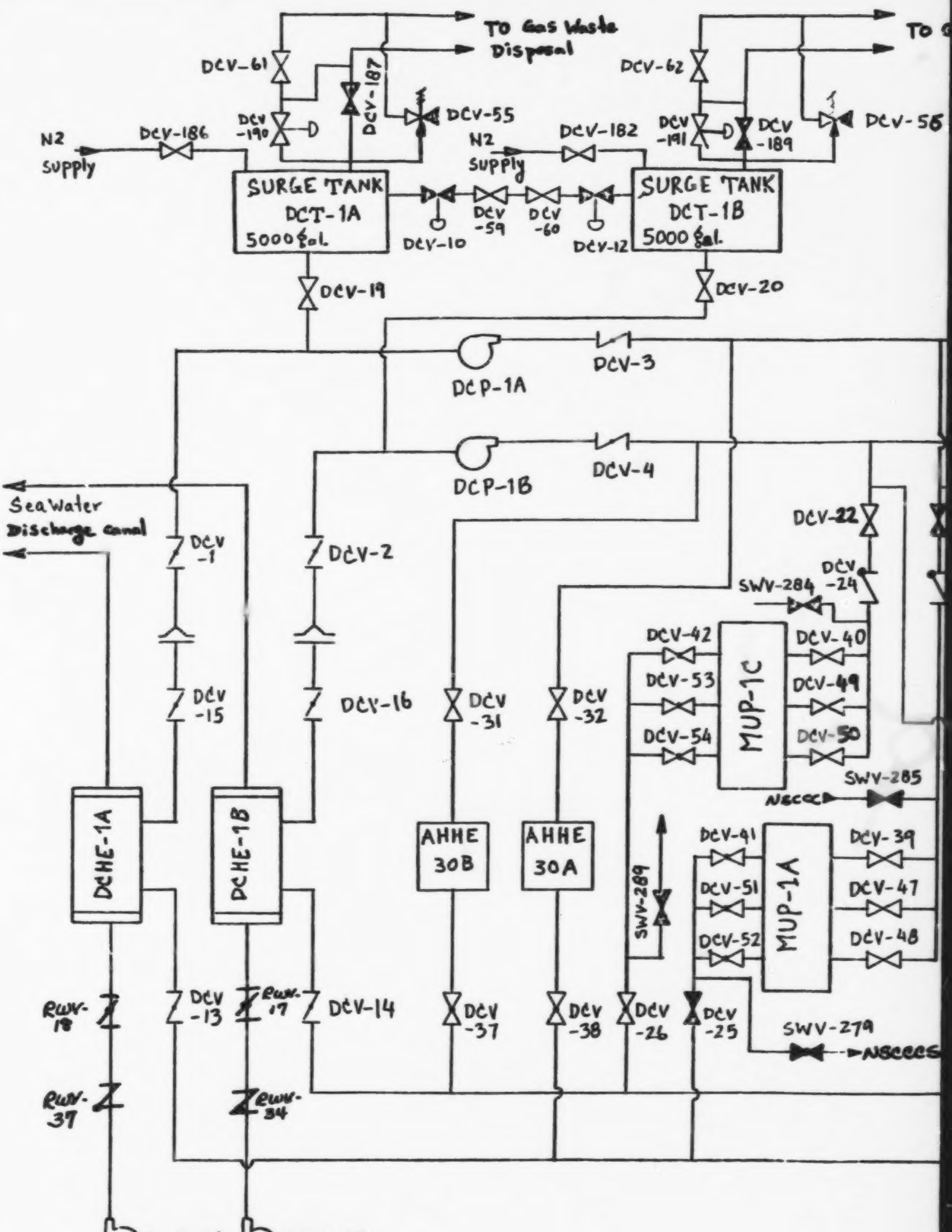
Decay Heat Closed Cycle Surge Tank

Number	2
Capacity, gal.	5000
Design Temperature, F	135
Design Pressure, psig	15
Material	Welded Carbon Steel
Code/Seismic Class	ASME Section VIII/I

Decay Heat Service Seawater Pumps

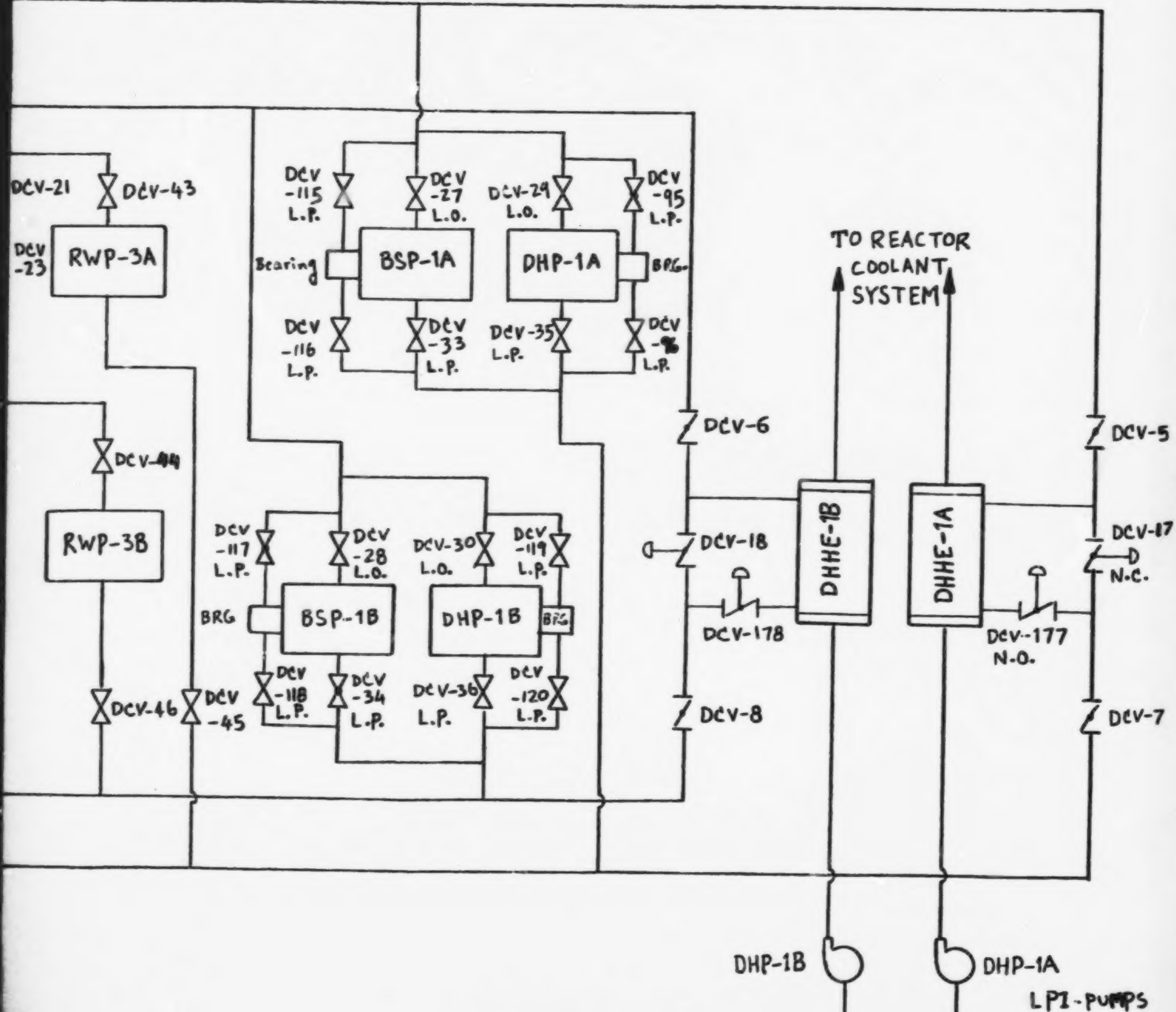
Number	2
Flow, gpm	9700
Design Head, ft	75
Design Pressure, psig	75
Design Temperature, F	109
Seismic Class	1

BEST DOCUMENT AVAILABLE


To Gas Waste Disposal
To
DCV-61
DCV-187
DCV-190
DCV-55
DCV-62
DCV-191
DCV-189
DCV-56
N2 supply
DCV-186
N2 supply
DCV-182
SURGE TANK DCT-1A 5000 gal.
SURGE TANK DCT-1B 5000 gal.
DCV-10
DCV-59
DCV-60
DCV-12
DCV-19
DCV-20
DCP-1A
DCV-3
DCP-1B
DCV-4
SeaWater Discharge canal
DCV-1
DCV-2
DCV-22
DCV-24
SWV-284
DCV-42
DCV-40
DCV-53
DCV-49
DCV-54
DCV-50
MUP-1C
DCV-15
DCV-16
DCV-31
DCV-32
SWV-285
NSCCC
DCHE-1A
DCHE-1B
AHHE 30B
AHHE 30A
SWV-289
DCV-41
DCV-39
DCV-51
DCV-47
DCV-52
DCV-48
MUP-1A
RWV-18
DCV-13
RWV-17
DCV-14
DCV-37
DCV-38
DCV-26
DCV-25
SWV-279
NSCCCS
RWV-37
RWV-34
RWP-3A
RWP-3B

as Waste Disposal

BEST DOCUMENT AVAILABLE


DCV-21
DCV-43
DCV -23
RWP-3A
DCV-44
RWP-3B
DCV-46
DCV -45
DCV -115 L.P.
DCV -27 L.O.
DCV-29 L.O.
DCV -95 L.P.
Bearing
BSP-1A
DHP-1A
BRG.
DCV -116 L.P.
DCV -33 L.P.
DCV-35 L.P.
DCV -96 L.P.
DCV -117 L.P.
DCV -28 L.O.
DCV-30 L.O.
DCV -119 L.P.
BRG
BSP-1B
DHP-1B
BRG
DCV -118 L.P.
DCV -34 L.P.
DCV-36 L.P.
DCV -120 L.P.
TO REACTOR COOLANT SYSTEM
DCV-6
DCV-18
DCV-178
DCV-8
DHHE-1B
DHHE-1A
DCV-5
DCV-17 N.C.
DCV-177 N.O.
DCV-7
DHP-1B
DHP-1A
LPI-PUMPS

215-A

Figure F.1 Decay Heat Closed Cycle Cooling System Schematic Diagram

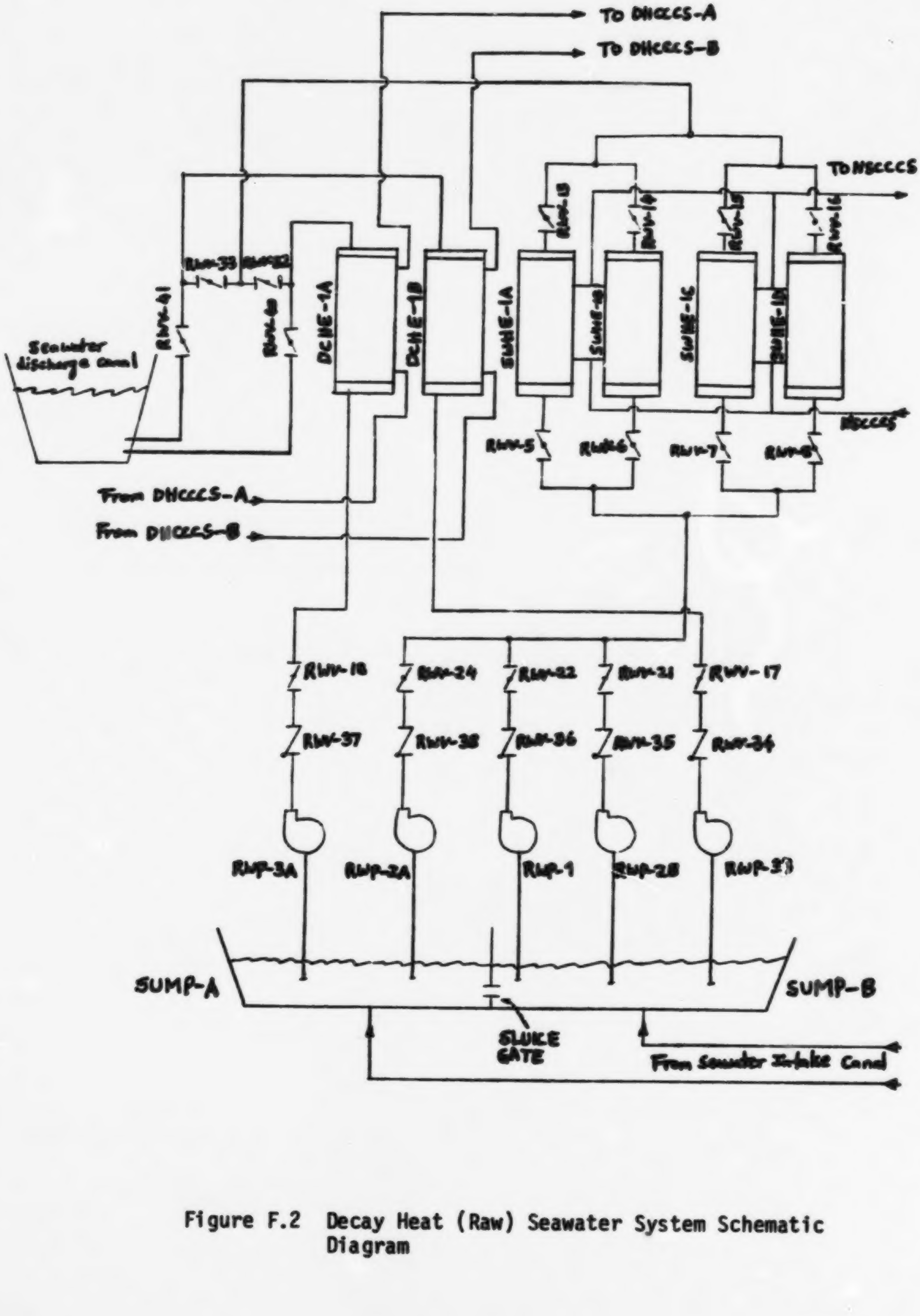

TO DHCCCS-A
TO DHCCCS-B
TO NSCCCS
RWV-13
RWV-14
RWV-15
RWV-16
RWV-39
RWV-32
RWV-41
RWV-40
Seawater discharge canal
DCHE-1A
DCHE-1B
SWHE-1A
SWHE-1B
SWHE-1C
SWHE-1D
NSCCCS
RWV-5
RWV-6
RWV-7
RWV-8
From DHCCCS-A
From DHCCCS-B
RWV-18
RWV-24
RWV-22
RWV-21
RWV-17
RWV-37
RWV-38
RWV-36
RWV-35
RWV-34
RWP-3A
RWP-2A
RWP-1
RWP-2B
RWP-3B
SUMP-A
SUMP-B
SLUICE GATE
From Seawater Intake Canal

Figure F.2 Decay Heat (Raw) Seawater System Schematic Diagram

F.2 SYSTEM SIMPLIFIED FAULT TREE

Figure F.3 is a simplified fault tree of the closed loop portion of DHCCCS Train A. The tree for failure of Train B is identical except for corresponding component number differences. Failure of flow in DHCCCS-A is a single fault for Train A of the Low Pressure and Containment Spray Systems. Failure of flow in DHCCCS-B will fail the analogous components, and in addition MUP-1C. There are additional faults which can cause cooling failure of components in the Low Pressure and Containment Spray Systems independently of the other components. These faults are primarily mispositioning of valves due to human error.

The major assumptions used to construct the simplified fault tree for DHCCCS-Train A (shown in Figure F.3) are listed below:

a. Components, lines, and valves that were considered insignificant contributors were omitted from the fault tree.

b. The DHCCCS is a normally inactive system. There is a probability it will be unavailable on demand due to maintenance, repair, or misposition of valves due to human error. There are no MOV's in the system. The manual block valves associated with each component are locally indicated and are not locked. Positions of valves in the flow path are checked once a month per SP-347. The only locked valves in the system are those on the cooling lines of DHP-1A, BSP-1A, and in the case of Train B, MUP-1C. Test frequencies are listed in the descriptive section. Each train is tested de facto, once every two weeks for three hours when the corresponding Decay Heating (LPI) pump is operated.

c. It was assumed that if flow to DHHE-1A was blocked, DCP-1A could still operate against the shut-off head, thus supplying bearing and motor cooling to the RWP-3A, BSP-1A, DHP-1A, and in the case of Train B, MUP-1C. Furthermore, it was assumed that failure to provide cooling for the pumps implies failure to provide cooling to DHHE-1A.

d. The system does not require reconfiguration for testing. It is, therefore, never unavailable due to periodic testing.

e. The gas pressure in the surge tank is not necessary for system operation. The intent is to prevent air bubbles from accumulating in the high points of the system. However, if the surge tank valve, DCV-19, is inadvertently closed, it was assumed that flow could not be established in the system.

f. All pumps can be started from the control room or at the breaker.

g. The Auxiliary Building which contains the closed cycle DHCCCS pumps, also contains the four nuclear service heat exchangers, the two DHCCCS heat exchangers, and three surge tanks. Common causative damage events could result in significant flooding of the room. This is a single fault for both DHCCCS pumps. However, the pump room is large and is equipped with a sump pump.

The major assumptions used to construct the simplified fault tree for the raw seawater portion of DHCCCS- Train A (shown in Figure F.3) are shown below:

a. Components, lines, and valves which were not considered significant were omitted from the analysis.

b. Loss of cooling to the bearing of RWP-3A is not considered significant for this study. The bearing pot is supplied by three sources. Cooling is accomplished by circulation of water through the bearing pot. The primary source of water is the domestic water system. The demineralized water system backs up the domestic water supply system. If both of these systems fail, the seawater will back into the bearing. This provides adequate cooling. It is not done on a permanent basis because it is undesirable from a corrosion standpoint.

c. The raw water loop of DHCCCS is a normally inactive system. There is a probability that it will be unavailable due to maintenance, repair, and mispositioning of valves.

d. Testing does not cause the system to be unavailable. Testing requires no reconfiguration. Test frequencies are stated in the descriptive section of this report. There are no locked valves in the system.

e. The pumps can be started from the control room or at the breaker.

f. Severe flooding of the pump room is a single fault which fails the pumps in both raw water trains.

g. Pump cavitation was considered unlikely enough to be ignored.

h. It was assumed the intake canal never goes dry while the plant is operating. T.S.3.4.7.5 limits the bottom of the canal to EL 74 and the minimum water level to EL 81. T.S.4.7.5.1 requires the inlet water temperature and water level to be checked every 24 hours It was further assumed the seawater sump never goes dry. Either section of the sump may be out of service at any given time for maintenance. There is a 48" pipe which gravity feeds the seawater sump from the intake structure. A separate pipe goes from the intake structure to each sump. A sluice gate also connects the two sumps. The canal is wide enough to preclude blockage by shipwreck. There are large grates on the intake structure which remove trash, seaweed, flotsam and jetsam from the seawater. It was assumed that blockage of these grates to the extent that they block flow is not possible.

i. OP-404 contains a procedure for the lay-up of the seawater side of DCHE-1A to prevent marine growth. This basically is a gravity drain and flush with domestic water. It involves opening and closing of drain valves, vent valves, and fill valves. Because these lines are very small, discharge rates would be very small if a valve was inadvertently left in the wrong position. For this reason, improper filling procedure was not considered a credible fault.

j. Due to its nature, the seawater system is exposed to a very corrosive-marine growth environment. Failures of the two seawater pumps were assumed to be coupled, as were failures of the two discharge check valves. Failure (plugging, blockage, marine-encrustation) of equipment in the dormant state was also considered. However, plugging and blockage of equipment while in operation was not considered likely.

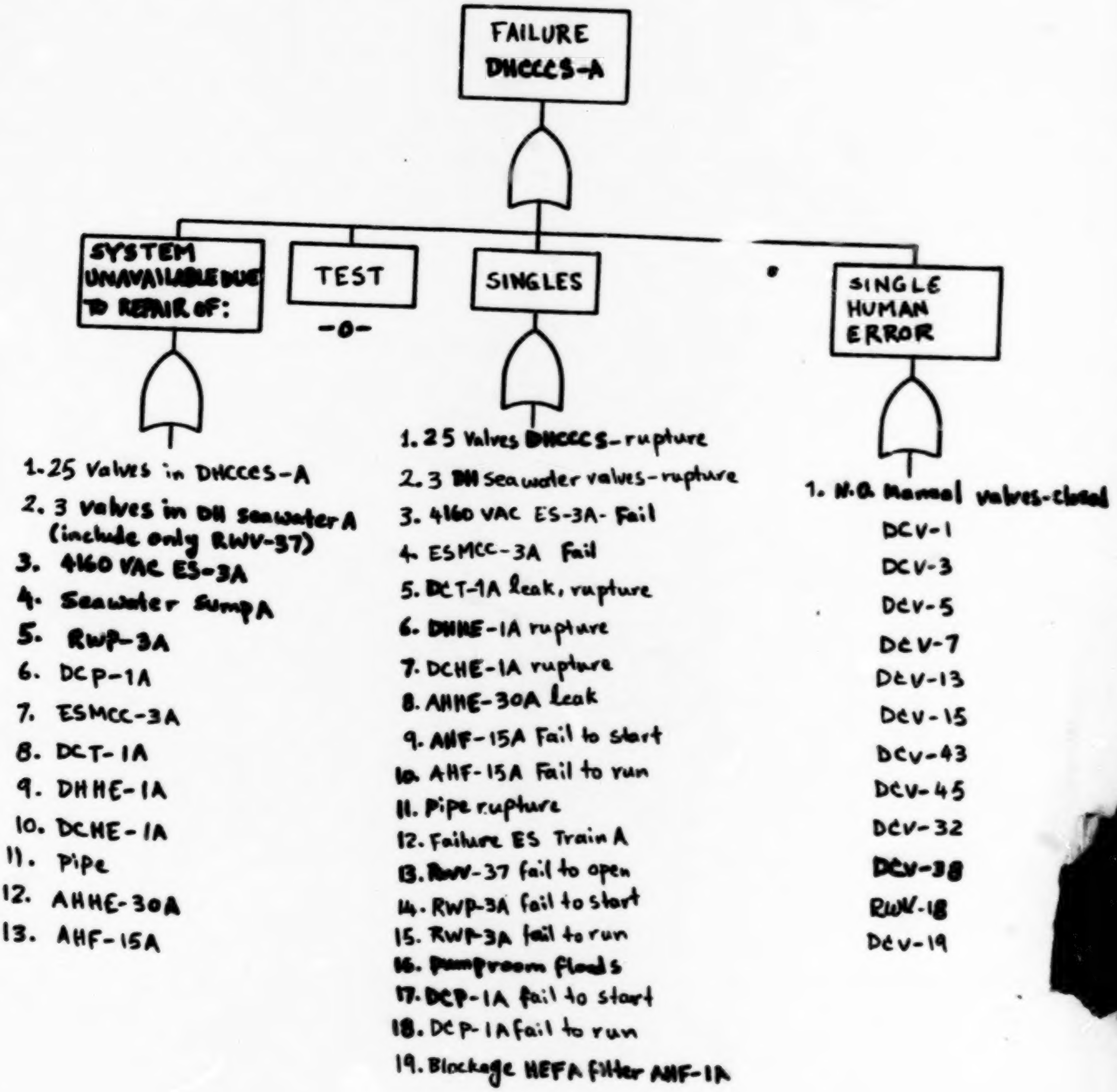

FAILURE
DHCCCS-A
SYSTEM
UNAVAILABLE DUE
TO REPAIR OF:
TEST
-0-
SINGLES
SINGLE
HUMAN
ERROR
1. 25 Valves in DHCCCS-A
2. 3 valves in DH seawater A (include only RWV-37)
3. 4160 VAC ES-3A
4. Seawater sump A
5. RWP-3A
6. DCP-1A
7. ESMCC-3A
8. DCT-1A
9. DHHE-1A
10. DCHE-1A
11. Pipe
12. AHHE-30A
13. AHF-15A
1. 25 Valves DHCCCS-rupture
2. 3 DH Seawater valves-rupture
3. 4160 VAC ES-3A- Fail
4. ESMCC-3A Fail
5. DCT-1A leak, rupture
6. DHHE-1A rupture
7. DCHE-1A rupture
8. AHHE-30A leak
9. AHF-15A Fail to start
10. AHF-15A Fail to run
11. Pipe rupture
12. Failure ES Train A
13. RWV-37 fail to open
14. RWP-3A fail to start
15. RWP-3A fail to run
16. Pumproom floods
17. DCP-1A fail to start
18. DCP-1A fail to run
19. Blockage HEPA filter AHF-1A
1. N.O. manual valves-closed
DCV-1
DCV-3
DCV-5
DCV-7
DCV-13
DCV-15
DCV-43
DCV-45
DCV-32
DCV-38
RWV-18
DCV-19

Figure F.3 Simplified Fault Tree - DHCCCS - Train A (including DHSS)

F.3 SYSTEM QUANTIFICATION

F.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The DHCCCS is a double train system with no cross-ties. This configuration allows failure of a single train to fail component cooling to the corresponding single train of several safety systems. Each train is dependent on the availability of AC power (AC power Train A powers DHCCCS Train A equipment and AC power Train B powers DHCCCS Train B equipment).

For cases where offsite power is available, the unavailability of a single train of DHCCCS was assessed to be principally due to single hardware faults, which were dominated by failure of the raw water pump, and to maintenance outages. The unavailability of both trains was assessed to be principally due to coupled raw water pump and check valve failure and maintenance outages coupled with failures on the in-service train.

For cases where offsite power is lost, diesel failures become dominant contributors to both single and double train DHCCCS failure, along with the same contributors described above. The unavailability of a single train of the DHCCCS for the loss-of-offsite power case is about a factor of three higher than the case where offsite power is available.

F.3.2 SYSTEM FAULT TREE QUANTIFICATION - INJECTION PHASE

This section presents the quantification of the DHCCCS unavailability for required emergency operation during the injection phase of a postulated accident. The quantitative results are presented in table form with attached notes outlining the assumptions. To perform the fault tree quantification, the simplified fault tree presented in Section F.3 was rearranged and is presented in this section in modular form.

Two modularized fault trees were constructed for the DHCCCS, one for failure of Train A and the other for failure of Train B. The failure of both trains is the product of these top events. In the new tree the product of two gates that were assumed to be coupled is treated as described in Section 4.1 of the Main Report.

Table F.2 shows the DHCCCS success requirements, Table F.3 contains the top event definitions for the two modularized fault trees, trees, and Figure F.4 shows the modularized fault trees for DHCCCS Trains A and B. The unavailability of each gate is shown on these as well as the top event unavailability. Table F.4 shows the Boolean equation that represents the fault trees. Table F.5 , the quantification tables, shows the quantification of each gate, by component and failure mode. The attached notes explain the assumptions used in the quantification. Table F.6 summarizes the point estimates for each gate, and the error factors that were used in the sensitivity analysis.

Table F.2 DHCCCS - System Success Requirements

INITIATOR	TRAINS	NOTES
B1, B2, B3, B4, transient initiators	Train A delivers one pump flow for component cooling and/or decay heat removal during injection.	1,2
	Train B delivers one pump flow for component cooling and/or decay heat removal during injection.	3

NOTES: 1. The DHCCCS is required for component cooling and/or decay heat removal for all LOCA sizes and transients requiring containment spray success.

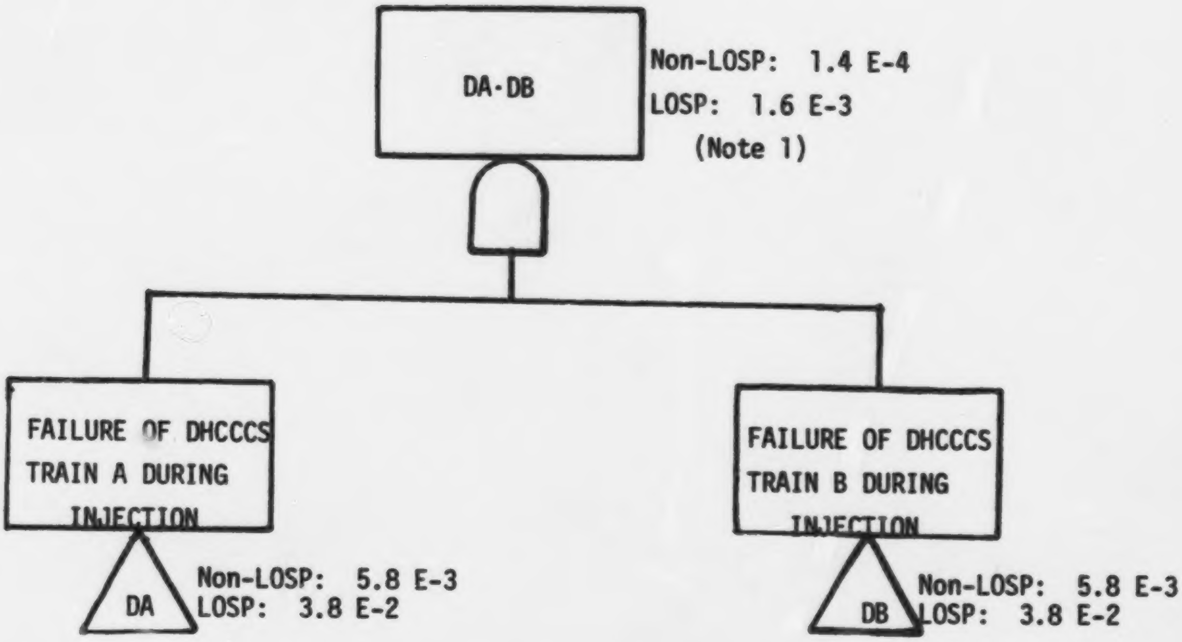
2. Train A of the DHCCCS supplies component cooling for containment spray pump BSP-1A, makeup pump MUP-1A, raw seawater pump RWP-3A, decay heat removal pump DHP-1A, and decay heat removal from low pressure Train A.

3. Train B of the DHCCCS supplies component cooling for containment spray pump BSP-1B, makeup pump MUP-1C, raw seawater pump RWP-3B, decay heat removal pump DHP-1B, and decay heat removal from low pressure Train B.

Table F.3 DHCCCS Top Event Definitions

BOOLEAN REPRESENTATION	TOP EVENT	NOTES
DA	Failure of DHCCCS Train A to provide one pump flow with ultimate heat removal for component cooling or decay heat removal during injection.	1
DB	Failure of DHCCCS Train B to provide one pump flow with ultimate heat removal for component cooling or decay heat removal during injection.	1

NOTE: 1. The event DA(DB) includes failures in both the closed cycle cooling system and the raw seawater system.


DA·DB
Non-LOSP: 1.4 E-4
LOSP: 1.6 E-3
(Note 1)
FAILURE OF DHCCCS TRAIN A DURING INJECTION
DA
Non-LOSP: 5.8 E-3
LOSP: 3.8 E-2
FAILURE OF DHCCCS TRAIN B DURING INJECTION
DB
Non-LOSP: 5.8 E-3
LOSP: 3.8 E-2

Note

1 Events DA and DB are not independent.

Figure F.4A Modularized Fault Tree for Event "DA·DB"

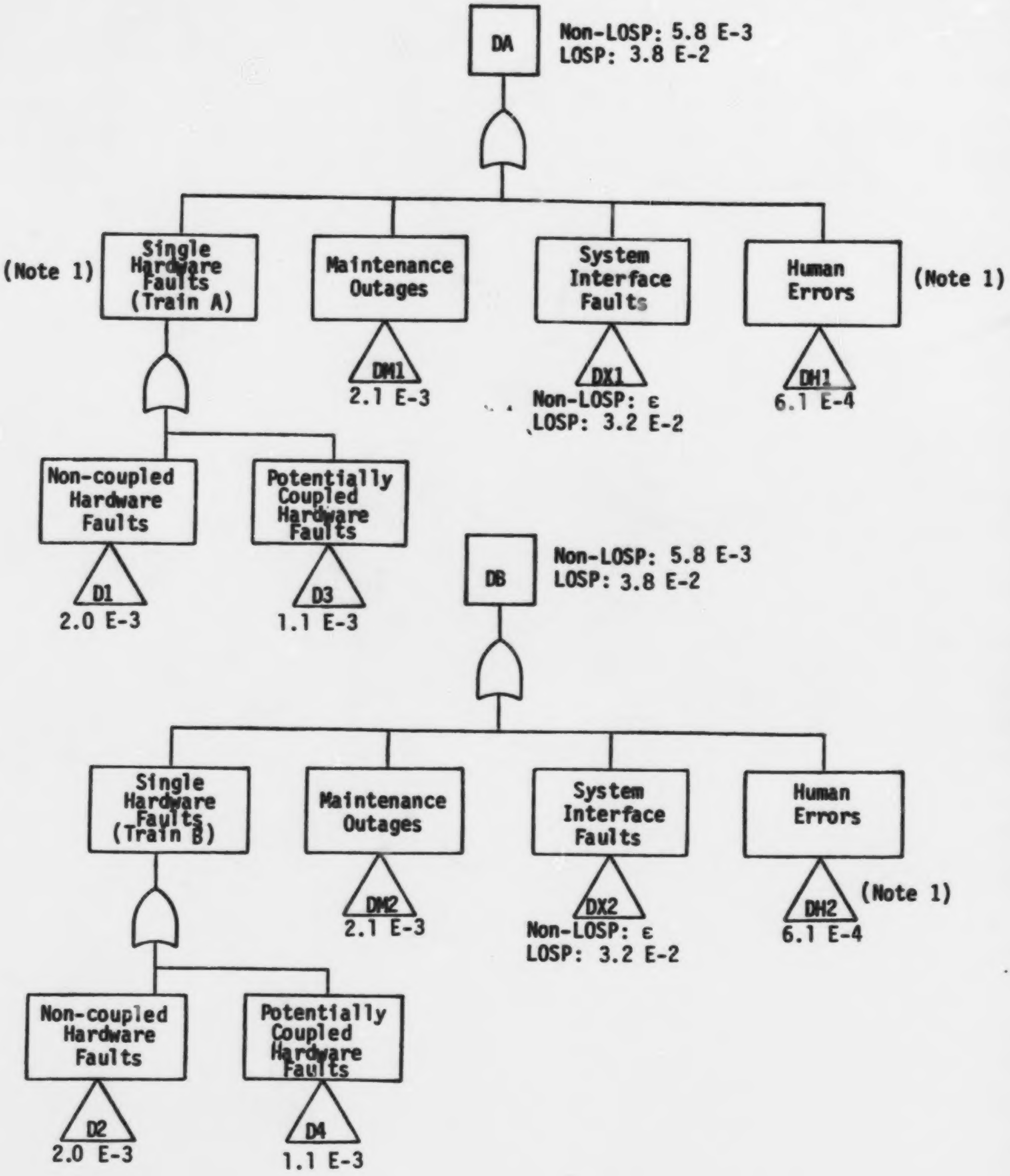

DA
Non-LOSP: 5.8 E-3
LOSP: 3.8 E-2
(Note 1)
Single Hardware Faults (Train A)
Maintenance Outages
System Interface Faults
Human Errors
(Note 1)
DM1
2.1 E-3
DX1
Non-LOSP: ε
LOSP: 3.2 E-2
DH1
6.1 E-4
Non-coupled Hardware Faults
Potentially Coupled Hardware Faults
D1
2.0 E-3
D3
1.1 E-3
DB
Non-LOSP: 5.8 E-3
LOSP: 3.8 E-2
Single Hardware Faults (Train B)
Maintenance Outages
System Interface Faults
Human Errors
DM2
2.1 E-3
DX2
Non-LOSP: ε
LOSP: 3.2 E-2
DH2
(Note 1)
6.1 E-4
Non-coupled Hardware Faults
Potentially Coupled Hardware Faults
D2
2.0 E-3
D4
1.1 E-3

Figure F.4 Modularized Fault Trees for Events "DA" and "DB"

Figure F.4 DHCCCS - Fault Trees

NOTES

1. Valve faults that would prevent component cooling to specific equipment are included in the fault tree analysis of the system in which the equipment is found.

Table F.4 DHCCCS - Injection

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP ENT	NOTES
$DA = D1 + D3 + DM1 + DX1 + DH1$	
$DB = D2 + D4 + DM2 + DX2 + DH2$	
$DA \cdot DB = D3 \cdot D4 + (D1 + DX1 + DH1) \cdot (D2 + D4 + DM2 + DX2 + DH2) + D3 \cdot (D2 + DM2 + DX2 + DH2) + DM1 \cdot (D2 + D4 + DX2 + DH2)$	1,2

INTERMEDIATE EVENTS	
$DX1 = ACA + DCA$	3
$DX2 = ACB + DCB$	3

NOTES: 1. Terms representing maintenance on both legs at the same time are deleted since this is prohibited by Technical Specifications.

2. The term D3·D4 represents component failures that were assumed to be coupled. See Quantification Tables.

3. DC power train failure is explicitly included in the Boolean equations. However, DC power train failure is also included in the failure of the AC trains, and will reduce out.

BEST DOCUMENT AVAILABLE

Table F.5 (1/3) Event "DA" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
D1		HARDWARE FAULTS THAT ARE NOT COUPLED WITH TRAIN B FAULTS			2.0 E-3			
	25 VALVES	RUPTURE			ε			1
	DCT-1A	SURGE TANK RUPTURE			ε			
	DHHE-1A	LOW PRESSURE SYSTEM HEAT EXCHANGER RUPTURE			ε			
	AHHE-3A	PUMP COOLING HEAT EXCHANGER RUPTURE			ε			
	AHF-15A	PUMP COOLING FAN FAILS TO START	D		3.0 E-4	$3^+, 3^-$		
	AHF-15A	FAILS TO RUN	1.0 E-5	10	1.0 E-4	$3^+, 3^-$		2
	PIPE	RUPTURES (SEVERAL SECTIONS)			ε			
	ESFAS A	FAILS TO INITIATE, AND OPERATOR FAILS TO RECOVER	(2.1E-4)(.1)		2.1 E-5			3,7
	PUMP RWP-3A	FAILS TO RUN	3.0 E-5	10	3.0 E-4	$10^+, 10^-$		2
	PUMP DCP-1A	FAILS TO START	D		1.0 E-3	$3^+, 3^-$		
	DCP-1A	FAILS TO RUN	3.0 E-5	10	3.0 E-4			2
	HEPA FILTER	PLUGGED			ε			
					Σ=2.0 E-3			
D3		HARDWARE FAULTS THAT ARE COUPLED WITH TRAIN B FAULTS			1.1 E-3	$3^+, 3^-$	S	
	CHECK VALVE RWV-37	FAILS TO OPEN	D		1.0 E-4	$3^+, 3^-$	S	
	PUMP RWP-3A	FAILS TO START	D		1.0 E-3	$3^+, 3^-$	S	
					Σ=1.1 E-3			
DM1		TRAIN A MAINTENANCE OUTAGE			2.1 E-3	$3^+, 3^-$	M	
	CHECK VALVE RWV-37	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	$3^+, 3^-$	M	
	PUMP RWP-3A	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	$3^+, 3^-$	M	
	PUMP DCP-1A	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	$3^+, 3^-$	M	
	AHF-15A	FAN OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	$3^+, 3^-$	M	
					Σ=2.1 E-3			
DX1		SYSTEM INTERFACE FAULTS						
ACA		AC TRAIN A						6
		NON LOSP			ε			
		LOSP			3.2 E-2			
DH1	HUMAN	6 OPPORTUNITIES TO LEAVE SINGLE VALVES CLOSED AFTER MAINTENANCE			6.0 E-4	$3^+, 3^-$	H	4

Table F.5 (2/3) Event "DB" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
D2		HARDWARE FAULTS THAT ARE NOT COUPLED WITH TRAIN A FAULTS			2.0 E-3			
	25 VALVES	RUPTURE			ε			
	DCT-1B	RUPTURE			ε			
	DHHE-1B	LOW PRESSURE HX-RUPTURE			ε			
	AHHE-30B	PUMP COOLING HEAT EXCHANGER			ε			
	AHF-15B	PUMP COOLING/FAN FAILS TO START	D		3.0 E-4	$3^+, 3^-$		
	AHF-15B	PUMP COOLING/FAN FAILS TO RUN	1.0 E-5	10	1.0 E-4	$3^+, 3^-$		2
	PIPE	RUPTURE (SEVERAL SECTIONS)	D		ε			
	ESFAS-B	FAILS TO INITIATE AND OPERATOR FAILS TO RECOVER	(2.1E-4)(.1)		2.1 E-5			3,7
	RWP-3B	RAW WATER PUMP FAILS TO RUN	3.0 E-5	10	3.0 E-4	$10^+, 10^-$		2
	DCP-1B	PUMP FAILS TO START			1.0 E-3	$3^+, 3^-$		
	DCP-1B	PUMP FAILS TO RUN	3.0 E-5	10	3.0 E-4	$10^+, 10^-$		2
	HEPA-FILTER	PLUGGED			ε			
					Σ=2.0 E-3			
D4		HARDWARE FAULTS THAT ARE COUPLED WITH TRAIN B FAULTS			1.1 E-3	$3^+, 3^-$	S	
	RWV-34	CHECK VALVE/FAILS TO OPEN	D		1.0 E-4	$3^+, 3^-$	S	
	PUMP RWP-3B	FAILS TO START	D		1.0 E-3	$3^+, 3^-$	S	
					Σ=1.1 E-3			
DM2		TRAIN B MAINTENANCE OUTAGE			2.1 E-3	$3^+, 3^-$	M	
	RWV-34	CHECK VALVE OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	$3^+, 3^-$	M	
	PUMP RWP-3P	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	$3^+, 3^-$	M	
	PUMP DCP-1B	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	$3^+, 3^-$	M	
	AHF-15B	OUT FOR MAINTENANCE	.02/720	19	5.3 E-4	$3^+, 3^-$	M	
					Σ=2.1 E-3			
DX2		SYSTEM INTERFACING FAULTS						
ACB		AC-TRAIN B						6
		NON LOSP			ε			
		LOSP			3.2 E-2			
DH2	HUMAN	6 OPPORTUNITIES TO LEAVE SINGLE VALVES CLOSED AFTER MAINTENANCE			6.0 E-4	$3^+, 3^-$	H	4

BEST DOCUMENT AVAILABLE

Table F.5 (3/3) Event "D3·D4" (Coupled Failure) Quantification for Failure of Both Trains

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
D3·D4		COUPLED FAILURES OF EQUIPMENT EXPOSED TO SEAWATER ENVIRONMENT			1.1 E-4	1^+, 10^-		5
	(RWV-34)	COUPLED SEAWATER CHECKVALVE FAILURES	(1.0 E-4)(0.1)		1.0 E-5	2^+, 2^-	B	
	(RWP-3A) x (RWP-3B)	COUPLED SEAWATER PUMP FAILURES	(1.0 E-3)(0.1)		1.0 E-4	2^+, 2^-	B	
					Σ=1.1 E-4	2^+, 2^-		

BEST DOCUMENT AVAILABLE

Table F.5 DHCCCS - Injection

QUANTIFICATION TABLES

NOTES

1 Rupture of any one of 25 separate valves in a single train of the DHCCCS was assessed to fail the system. These valves each see surge tank system pressure. However, rupture of any of the valves would drain the surge tank which is monitored. Therefore, these faults are assessed to be ϵ.

2 The DHCCCS is required for all LOCA-sizes and transients. The injection period depends on the LOCA size or transient duration (0.5 to 10 hours). The fault duration time was conservatively chosen for the 10 hour injection period.

3 The failure of ESFAS to actuate single equipment was assessed as 2.1 E-4 (Event ISS1 in ESAS quantification). This number is applicable for a B4 LOCA and would be smaller for the other LOCA cases; however, it is an insignificant contributor and was therefore not changed for the larger LOCAs. Failure to recover was assumed to be 0.1 per act.

4 Each opportunity to leave a valve open is associated with isolation of active components during maintenance. When more than one valve is involved with the maintenance activity on a single component, they are treated collectively as providing one opportunity for inadvertent closure. The valve combinations for Train A are: DCV-1, -3 and -19 (for DCP-1A); DCV-5 and -7 (for DHHE-1A); DCV-13 and -15 (for DCHE-1A); DCV-43 and -45 (for RWP-3A); DCP-32 and -38 (for AHHE-30A); and RWV-18 (for RWP-3A). Similar combinations apply to Train B. This fault was assessed assuming a human error probability of 1.0 E-2 for leaving closed after maintenance any of the valves associated with one component. The frequency at which this could occur was assumed to be 0.02 times per month. However, because the decay heat system is tested once every 2 weeks, the fault duration time was assessed as 1/2 month. The fault was assessed as 6 opportunities times 0.02 times 1/2 times 1.0 E-2.

5 The seawater check valves and pumps in Trains A and B were assumed coupled with a β-factor of 0.1.

6 Only AC power faults are involved, although DC power is required to close breakers that start pumps. DC power train failures are included in the AC fault tree, and would Boolean reduce out of the gate for system interface faults. Therefore, it would not be appropriate to add the AC and DC unavailability to obtain the system interface gate unavailability.

Table F.5 DHCCCS - Injection

QUANTIFICATION TABLES (NOTES) continued

7 Failure of ESAS to provide actuation signals to both trains is not included because the potential for recovery is high enough to make this contribution negligible.

Table F.6 DHCCCS - Injection Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
D1	2.0 E-3
D3	1.1 E-3
DM1	2.1 E-3
ACA	ε* 3.2 E-2**
DH1	6.0 E-4
D2	2.0 E-3
D4	1.1 E-3
DM2	2.1 E-3
ACB	ε* 3.2 E-2**
DH2	6.0 E-4
D3·D4	1.1 E-4

*Offsite power available
**Offsite power not available

F.3.3 SYSTEM FAULT TREE QUANTIFICATION - RECIRCULATION PHASE

This section presents the quantification of the DHCCCS unavailability for required emergency operation during the recirculation phase of a postulated accident. As in the injection case, modularized fault trees were constructed for failure of Train A and failure of Train B. Failure of either train during the recirculation phase is predicated on success during the injection phase; if a train fails during injection, it is assumed to be unavailable for recirculation. Thus, only DHCCCS hardware failures that occur during recirculation are assumed to contribute to the top events.

Table F.7 shows the DHCCCS success requirements, Table F.8 contains the top event definitions, and Figure F.6 shows the modularized fault trees for failure of Train A and B, respectively. The unavailability of each gate is shown in these trees, as well as the top event unavailabilities. Table F.9 shows the Boolean equations that represent the fault trees. Table F.10, the quantification table, shows the quantification of each gate, by component and failure mode. The attached notes to this table outline the assumptions used in the quantification. Table F.11 summarizes the point estimates for each gate.

Table F.7 DHCCCS - System Success Requirements - Recirculation

INITIATOR	TRAINS	NOTES
B1, B2, B3, B4, transient initiators	Train A delivers one pump flow for component cooling and/or decay heat removal during recirculation.	1,2,4
	Train B delivers one pump flow for component cooling and/or decay heat removal during recirculation.	3,4

NOTES: 1. The DHCCCS is required for component cooling and/or decay heat removal for all LOCA sizes and transients requiring containment spray success.

2. Train A of the DHCCCS supplies component makeup pump MUP-1A, raw water pump RWP-3A, decay heat removal pump DHP-1A, and decay heat removal from low pressure Train A.

3. Train B of the DHCCCS supplies component cooling for containment spray pump BSP-1B, makeup pump MUP-1C, raw water pump RWP-3B, decay heat removal pump DHP-1B, and decay heat removal from low pressure Train B.

4. Recirculation phase is assumed to last for 24 hours after injection phase.

Table F.8 DHCCCS Top Event Definitions - Recirculation

BOOLEAN REPRESENTATION	TOP EVENT	NOTES
DA*	Failure of DHCCCS Train A to provide one pump flow with ultimate heat removal for component cooling or decay heat removal during recirculation.	1,2
DB*	Failure of DHCCCS Train B to provide one pump flow with ultimate heat removal for component cooling or decay heat removal during recirculation.	1,2

NOTES: 1 The event DA*(DB*) includes failures in both the closed cycle cooling system and the raw water system.

2. Assumes success during injection phase.

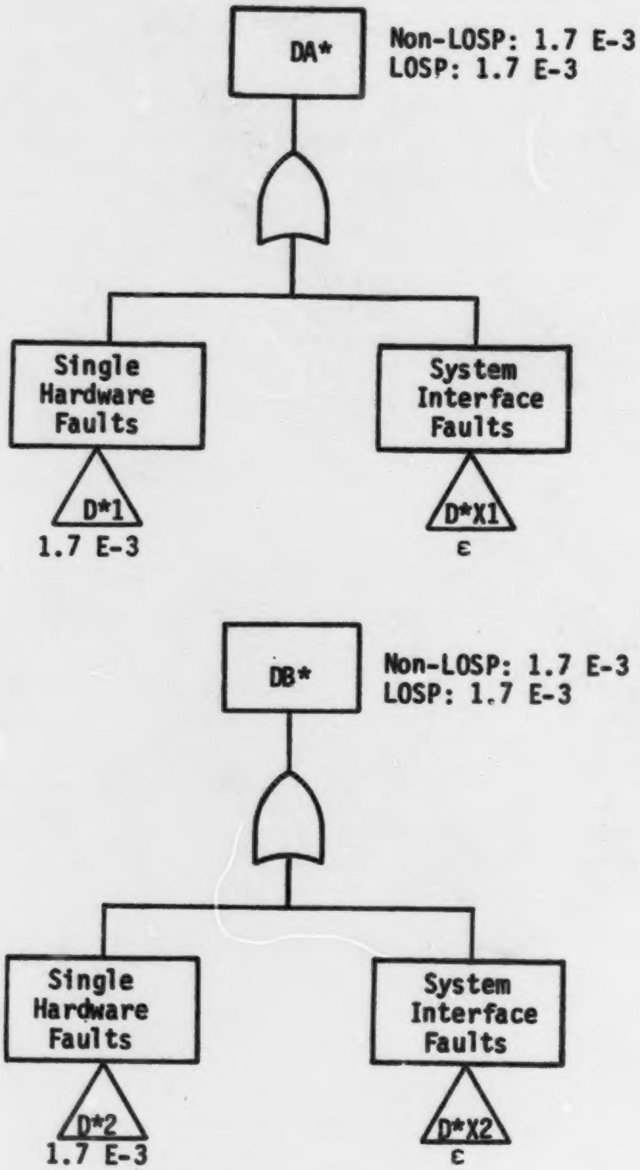

DA*
Non-LOSP: 1.7 E-3
LOSP: 1.7 E-3
Single Hardware Faults
System Interface Faults
D*1
1.7 E-3
D*X1
ε
DB*
Non-LOSP: 1.7 E-3
LOSP: 1.7 E-3
Single Hardware Faults
System Interface Faults
D*2
1.7 E-3
D*X2
ε

Figure F.5 Modularized Fault Tree for Events "DA*" and "DB*"

Table F.9 DHCCCS - Recirculation

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS	NOTES
DA* = D*1 + D*X1	
DB* = D*2 + D*X2	
INTERMEDIATE EVENTS	
D*X1 = ACA*	1
D*X2 = ACB*	1

NOTES: 1. Offsite power is assumed to be recovered when entering the recirculation phase. The unavailability of AC power with offsite power available was calculated to be negligible compared to other system failure modes.

BEST DOCUMENT AVAILABLE

Table F.10 Events "DA*" and "DB*" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
D*1		HARDWARE FAULTS THAT OCCUR DURING RECIRCULATION - TRAIN A			1.7 E-3			
	FAN HAF-15A	FAILS TO RUN	1.0 E-5	24	2.4 E-4	3^+, 3^-		
	PUMP RWP-3A	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10^+, 10^-		
	PUMP DCP-1A	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10^+, 10^-		
					Σ=1.7 E-3			
D*X1		SYSTEM INTERFACE FAULTS			ε			
ACA*		AC TRAIN A						
		FAILS DURING RECIRCULATION			ε			
		NON LOSP			ε			
		LOSP			ε			
D*2		HARDWARE FAULTS THAT OCCUR DURING RECIRCULATION - TRAIN B			1.7 E-3			
	FAN AHF-15B	FAILS TO RUN	1.0 E-5	24	2.4 E-4	3^+, 3^-		
	PUMP RWP-3B	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10^+, 10^-		
	PUMP DCP-1B	FAILS TO RUN	3.0 E-5	24	7.2 E-4	10^+, 10^-		
					Σ=1.7 E-3			
D*X2		SYSTEM INTERFACE FAULTS			ε			
ACB*		AC TRAIN B						
		FAILS DURING RECIRCULATION			ε			
		NON LOSP			ε			
		LOSP			ε			

Table F.11 DHCCCS - Recirculation Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
D*1	1.7 E-3
D*X1	ε
ACA*	ε
D*2	1.7 E-3
D*X2	ε
ACB*	ε

APPENDIX G

HIGH PRESSURE INJECTION AND RECIRCULATION SYSTEM

APPENDIX G HIGH PRESSURE INJECTION AND RECIRCULATION SYSTEM

G.1 SYSTEM DESCRIPTION AND OPERATION

The HP-system is used to provide emergency coolant to the reactor vessel in the event of a small loss of coolant accident where the reactor coolant system (RCS) is not depressurized sufficiently for core flood or for low pressure coolant injection. The High Pressure Injection (HPI) is also used to delay the need for core flood and low pressure coolant injection in the event of intermediate size RCS breaks.

The HP-system is required to operate during both the injection (HPI configuration) and recirculation (HPR-configuration) phases of small LOCAs and transients. It also provides an alternate to the Emergency Feedwater System for core cooling during loss of feedwater transients, when the EFS is not available (referred to as "Feed and Bleed" operation). The HP-system is an operating mode of the makeup and purification system, and consists of a portion of that operating system, with additional standby components.

G.1.1 SYSTEM DESCRIPTION

The HP-system is comprised of the pumps, valves, storage tank and interconnecting piping shown in Figure G.1. Although three pumps and four injection valves are shown, the system is essentially a two-train system because of its interfaces with other systems. These interfaces are summarized as follows:

(1) Borated Water Storage Tank (BWST) - common to both trains.

(2) Engineered Safeguards Actuation System (ESAS)

ESAS-A - Starts Pumps 1A and 1B
Closes Valves 27, 53, 64
Opens Valves 23, 24, 73

ESAS-B - Starts Pump 1C
Closes Valves 64, 257
Opens Valves 25, 26, 58

(3) AC Power

4160V Bus 3A - Pumps 1A and 1B
4160V Bus 3B - Pump 1C
480V MCC 3A1 - Valves 23, 24, 27, 53, and 73
480V MCC 3B1 - Valves 25, 26, and 257

(4) DC Power

125VDC A - Pumps 1A and 1B
Valve 64
125VDC B - Pump 1C
Valve 64

(5) Nuclear Services Closed Cycle Cooling System (NSCCCS)
- Cools Pumps 1A and 1B

(6) Decay Heat Closed Cycle Cooling System (DHCCCS)
- Cools Pump 1C

The Crystal River HP-system contains the following features:

- Pump 1B can be shifted from Train A to Train B by manually shifting its circuit breaker from its Bus 3A cubicle to its Bus 3B cubicle.
- Valve 64 isolates HPI from the makeup tank. It gets signals to close from both ESAS trains, and it obtains control power from both 125VDC trains.
- Should loss of power occur on 480VAC Train A, injection valves can be switched manually in the control room to Train B; likewise, injection valves 25 and 26 can be switched to Train A upon loss of Train B power. Loss of 480 VAC power on either train should be readily apparent in the control room.
- The cooling water to pumps 1A and 1C can be changed by realignment of valves to the DHCCCS or NSCCCS systems, respectively. Pump 1B is always cooled by NSCCCS. The lineup of cooling water systems with HPI pumps has been changed to that indicated above and does not agree with the Crystal River Final Safety Analysis Report.

Most of the HP-system components are located inside the auxiliary building adjacent to the reactor building. Exceptions are the borated water storage tank which is located outside adjacent to and south of the reactor building and check valves 36, 37, 42, 43, 160, 161, 163, and 164 which are located in the injection lines inside the reactor building. The pumps are located in an auxiliary building room adjacent to and east of the reactor building. These pumps are separated from each other by concrete walls which serve as missile shields.

The following is a summary description of the major components in the HPI system.

BWST

Capacity	420,000 gal.

Pumps

Type	Horizontal, Multistage Centrifugal, Mechanical Seal
Rated Capacity @ 2400 psi	300 gpm
Rated Head	5,545 ft.
Motor Size	700 hp
Design Pressure	3000 psig
Design Temp	200°F
Speed	6800 rpm

Each pump is equipped with two lube oil pumps (one AC and one DC) and two gear oil pumps (one AC and one DC). Upon loss of an AC pump, or its power source, the DC alternate pump starts automatically. The AC and DC lube and gear oil pumps are aligned to Train A or Train B power sources in concert with their associated HPI pump lineup.

Valves

All valves are Seismic Class I conforming to ASME III requirements.

G.1.2 SYSTEM OPERATION

HPI is initiated automatically by the engineered safeguards actuation system (ESAS) upon 1500 psig decreasing RCS pressure, 500 psig RCS pressure, or 4 psig increasing reactor building pressure. The system can also be started manually. During normal reactor operation the system draws treated water from a makeup tank using one pump (usually 1B) and discharges that water into RCS loop 3A1 (via control valve 31 and block valve 27 as shown in Figure G.1). The system also provides seal water to the RCS pumps. Upon receipt of an ESAS signal the system is realigned so that coolant is drawn from the borated water storage tank (BWST) by three pumps (two pumps if only diesel power is available) and is discharged through four injection lines into the four RCS cold legs, respectively. The makeup tank and the normal makeup and seal water discharge paths are isolated upon HPI.

Once started by the ESAS the operator cannot reconfigure the system without first bypassing those ESAS channels which initiated HPI. This includes such subsequent reconfiguration as valve realignment for recirculation of spilled fluid from the reactor building sump and injection valve throttling to limit pump flow or coolant loss through a RCS break. All of these reconfigurations are required by procedures. Once valves are reconfigured or pumps stopped they are subject to becoming commanded back to the injection mode by subsequent ESAS signals; e.g., by the 4 psig reactor building pressure signal if not also bypassed.

The following summarizes the operational sequence of the HPI:

- Pump 1B or 1A normally running with injection via makeup line.
- Figure shows normal valve lineup with either pump 1A or 1B running.
- HPI automatically actuated by ESAS on low RCS pressure (∿ 1500 psi).
- Actuation starts all pumps, opens injection valves 23F, 24F, 25F, 26F; opens valve 73, sends open signal to MV 58 (normally open); closes makeup valve 27, closes recirculation valves 257 and 53, closes makeup suction valve 64.

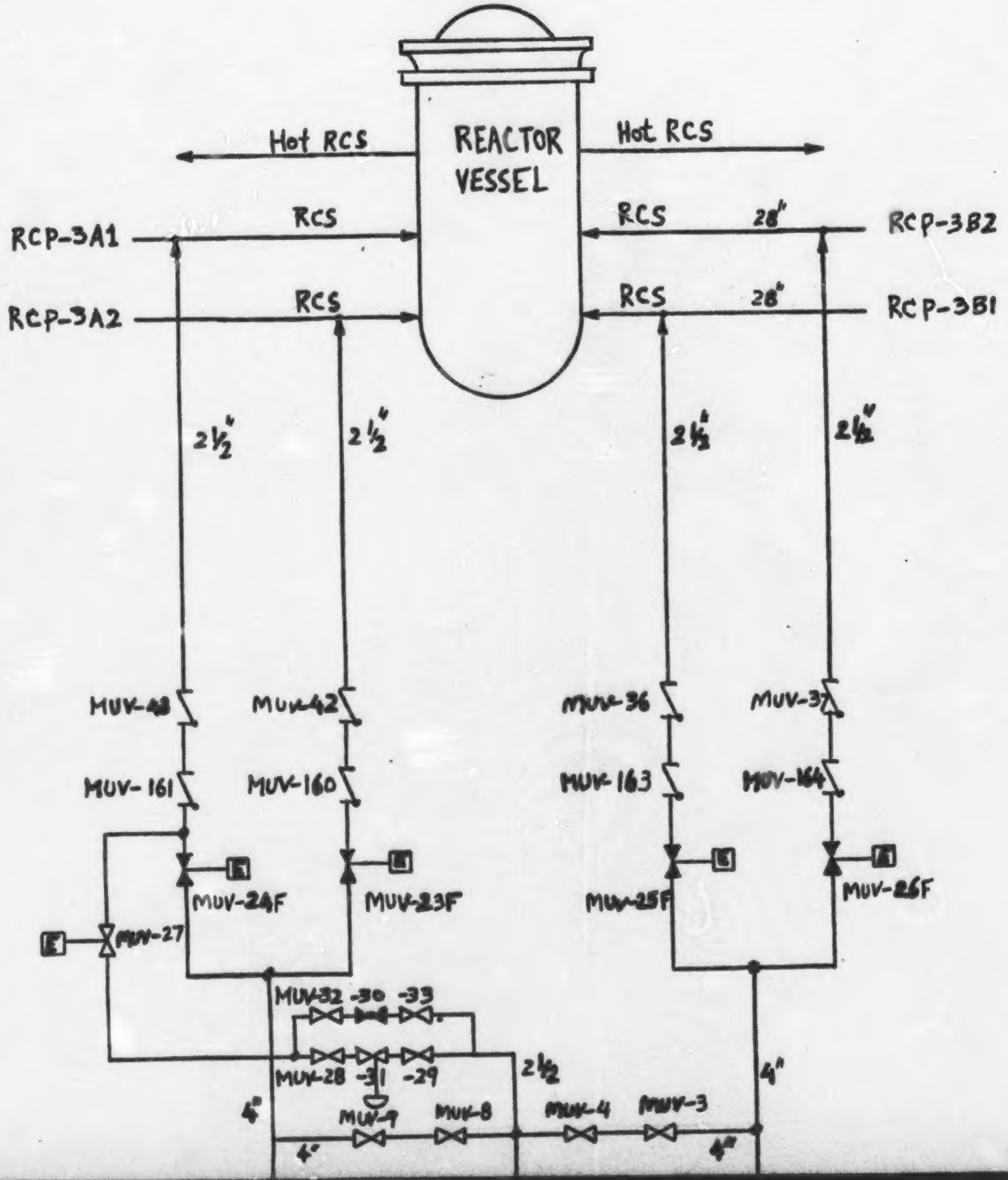
- Some small breaks in the injection line require isolation of the affected line by closing the injection valve. Operator must bypass HPI/ESAS channel to close the valve.
- Procedures (EP-106) call for controlling flow by throttling injection valves. Requires bypassing HPI/ESAS channels A and B.

The HPI pumps are tested by running them alternately for approximately one hour each month. All valves that must respond to an accident are fully or partially stroked once each quarter. Pump and valve tests do not alter the system such that it or its subsystems would be unavailable upon demand.

No maintenance is performed on the system unless a component has failed or the reactor is shut down. Technical specifications require that at least two HPI pumps be operable. If only one pump is operable another pump must be restored within 72 hours, or the plant must be placed in hot standby within six hours. If at hot standby and only one pump is operable, another pump must be restored to operable status within the next seven days, or the plant must be in cold shutdown within 30 hours.

All motor operated valves and pumps can be operated using switches in the control room. Manual valves are locked in position using padlocks.

BEST DOCUMENT AVAILABLE


REACTOR
VESSEL
Hot RCS
Hot RCS
RCP-3A1
RCP-3A2
RCS
RCS
RCS
RCS
28"
28"
RCP-3B2
RCP-3B1
2½"
2½"
2½"
2½"
MUV-43
MUV-42
MUV-36
MUV-37
MUV-161
MUV-160
MUV-163
MUV-164
E
E
E
E
MUV-24F
MUV-23F
MUV-25F
MUV-26F
E
MUV-27
MUV-32 -30 -33
MUV-28 -31 -29
2½
4"
4"
MUV-9
MUV-8
MUV-4
MUV-3
4"
4"

BEST DOCUMENT AVAILABLE

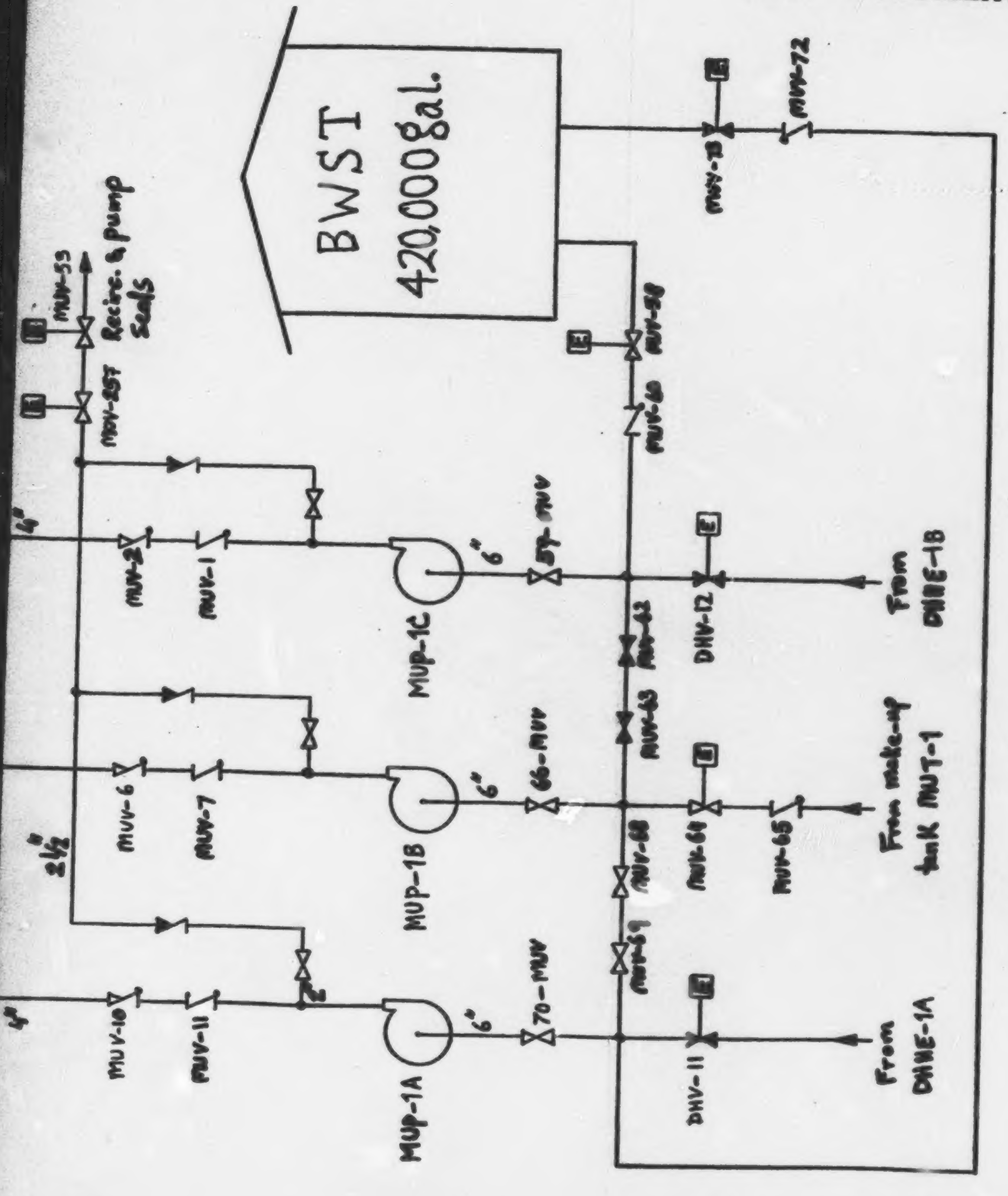

BWST
420,000 gal.
MUV-55
Recirc. & Pump Seals
MUV-257
MUV-73
MUV-72
MUV-58
MUV-60
4"
MUV-2
MUV-1
MUP-1C
6"
57-MUV
MUV-62
DHV-12
From DHHE-1B
MUV-6
MUV-7
2½"
MUP-1B
66-MUV
MUV-63
MUV-68
MUV-64
MUV-65
From make-up tank MUT-1
4"
MUV-10
MUV-11
2"
MUP-1A
70-MUV
MUV-69
DHV-11
From DHHE-1A
E

Figure G.1 High Pressure Injection System Schematic Diagram

G.2 SIMPLIFIED FAULT TREE

Two fault trees were developed: one tree for the accident initiating events that require only one-pump flow and another tree for those accident initiators that require two-pump flow. However, the fault tree for the two pump flow case was not evaluated, since:

- Two pump flow is required for ATWS, but ATWS was estimated to be a very low probability event, and ATWS sequences were not evaluated in this study.
- The break size requiring two pump flow (between 0.008 ft^2 and 0.015 ft^2) will result in some core damage if only one pump is operating, but not core melt.*

For these reasons only the fault tree resulting from one pump flow success criteria was evaluated. The simplified form of this fault tree is shown in Figure G.2. The fault tree was developed using information contained in the Crystal River, Unit 3, Final Safety Analysis Report, system drawings (primarily FD-302-661), plant procedures and correspondence, and from plant visits. The simplified form of the fault tree shows only the single passive and active faults and the double active faults. All higher order combinations of component faults were considered to be negligible contributors to system failure probability. Human error events are also shown on the fault tree.

Success/Failure Criteria. One of three HPI pumps is required for all RCS breaks, or for a stuck open power operated relief valve (PORV). Two of three available injection lines were considered successes on the fault tree. One of four injection lines was assumed to be unavailable for injection because of the initiating event. If the break (or initiating event) occurs in the RCS recirculation loop, no credit is given for coolant injection into the broken loop. If the break occurs in the injection line itself (between the block valve and the RCS loop) the block valve must be closed by the operator.

---

*Telecon 11/16/79 with R. Jones, B&W

Assumptions. Assumptions and ground rules used in the development of the fault tree are as follows:

(1) Breaks in the RCS which require HPI flow were assumed to be in the cold leg of RCS loop 3B1. Loss of coolant from this loop is somewhat more likely because a stuck open PORV and an open pressurizer spray valve would result in coolant loss from RCS loop 3B1. Failure of valves to open in this injection loop do not appear as faults on the fault tree. The flow requirements for success assume that part of the fluid will be discharged out the break, therefore, success does not depend upon isolation of the break by closing block valve 25.

(2) HPI injection line breaks were assumed to occur in the line to RCS loop 3B1. It was assumed that a break in any of the four injection lines was equally likely, and therefore the selection would have no bearing on the numerical results. If a break occurs in an injection line it is incumbent on an operator to close the associated block valve; otherwise insufficient coolant will be delivered to the RCS despite the number of operating HPI pumps.

(3) Isolation of the pump recirculation and RCS pump seal water piping was assumed necessary in order to assure that all flow is injected into the RCS. (Isolation is certainly important from a containment integrity point of view during recirculation. If not isolated, contaminated water would be pumped to the makeup tank and ultimately released to the atmosphere).

(4) Pump 1B is the pump normally used for RCS coolant makeup. It was acknowledged on the fault tree that this pump might be down for maintenance because of its required long duty cycle (high likelihood of malfunctioning). If pump 1B is down, pump 1A was assumed to be operating as a makeup pump at the time of the accident.

It was assumed that pump 1B is aligned to the Train A services at the time of an accident and that it cannot be be changed during the course of an accident. Changeover would require a shifting of pump 1B breaker at the switchgear.

(5) It was assumed that the system must be started automatically following an accident. This is to say that the operator expects that it will start and if it doesn't start it is too late for the operator to do so. (This is a conservative assumption and may not be a realistic one).

Table G.1 (1/2) High Pressure System Fault Summary

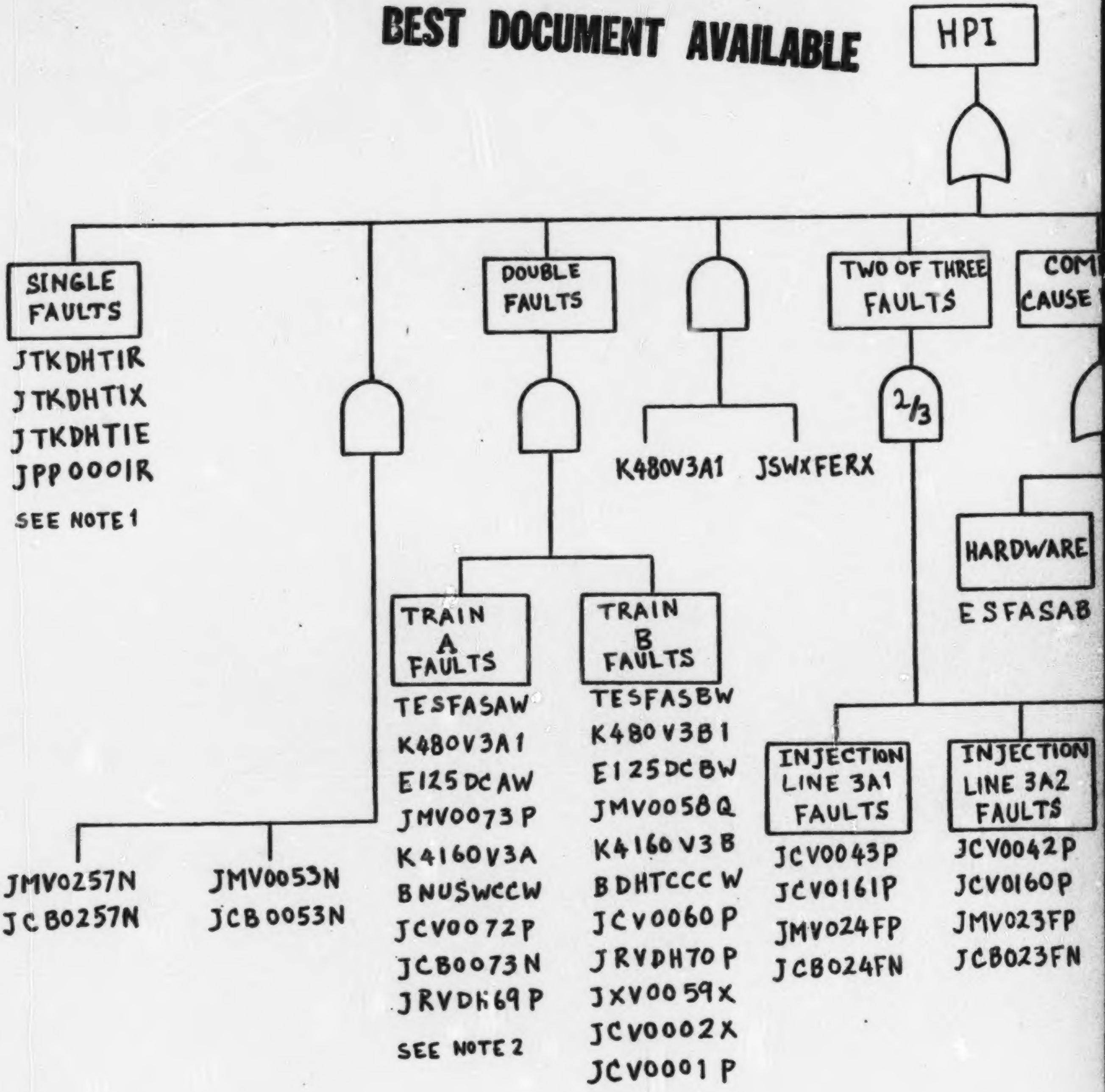
SIMPLIFIED FAULT TREE - FAULT SUMMARY

EVENT NAME	EVENT COMPONENT	FAILURE MODE
JCV0042P	Check Valve 42	Does Not Open
JCV0160P	Check Valve 160	Does Not Open
JMV023FP	Motor Operated Valve 23F	Does Not Open
JMV0073P	Motor Operated Valve 73A	Does Not Open
JCV0072P	Check Valve 72	Does Not Open
JCV0010P	Check Valve 10	Does Not Open
JCV0011P	Check Valve 11	Does Not Open
JPM001AS	Pump 1A	Does Not Start
JPM001AR	Pump 1A	Stops Running
JXV0070X	Manual Valve	Left Closed
JCV0010X	Stop Check Valve	Left Closed
JPM001BQ	Pump 1B	Out of Service
E125DCBW	125VDC Bus B	No Output
JCV0036P	Check Valve 36	Does Not Open
JCV0163P	Check Valve 163	Does Not Open
JMV024FF	Motor Operated Valve 245	Does Not Open
JCV0037P	Check Valve 37P	Does Not Open
JCV0164P	Check Valve 164	Does Not Open
JMV026FP	Motor Operated Valve 26F	Does Not Open
JCV0001P	Check Valve 1	Does Not Open
JCV0002P	Check Valve 2	Does Not Open
JXV0059X	Manual Valve 59	Left Closed
JCV0060P	Check Valve 60	Does Not Open
JMV0058Q	Motor Operated Valve 58	Does Not Remain Open
E125DCAW	125VDC Bux A	No Output
JTKDHT1R	Rank DHT-1 (RWST)	Rupture
JPM001CS	Pump 1C	Does Not Start
JPM001CR	Pump 1C	Stops Running
BNUSWCCW	Nuclear Service Water System	No Cooling Water to Pump 1B
JTKDHT1X	BWST	Not Full
K4160V3A	4160VAC Bus 3A	No Power to Pump 1B
K480V3A1	480VAC Bus 3A1	No Power to Valves
TESFASAW	Engineered Safeguards Actuation System A	No Signal to Start HPI-A
BDHTCCCW	Decay Heat Closed Cycle Cooling	No Cooling to Pump 1C
JTKDHT1E	BWST Output Piping	Plugged
K4160V3B	4160VAC Bus 3B	No Power to Pump 1C

Table G.1 (2/2) High Pressure System Fault Summary

SIMPLIFIED FAULT TREE - FAULT SUMMARY		
EVENT NAME	EVENT COMPONENT	FAILURE MODE
K480V3B1	480VAC Bux 3B1	No Power to Valves
TESFASBW	Engineered Safeguards Actuation System B	No Signals to HPI B
JXX0001X	Operator Error	System Stopped Prematurely
JPP0001R	Any Pipe Between DHT-1 and Injection Valve	Rupture
JXX0002X	Valve 59 (for isolating pumps 1A & 1C)	Left Closed After Maintenance
JMV0025V	Broken Loop Not Isolated by Operator	
JSWXFERX	480V Power to Injection Valves 23F and 24 F XFER Switch	Operator Does Not XFER
JCB001AN	Motor Starter for Pump 1A	Does Not Close
JCB001CN	Motor Starter for Pump 1C	Does Not Close
JCB024FN	Motor Starter for Valve 24E	Does Not Close
JCB023FN	Motor Starter for Valee 23F	Does Not Close
JCB026FN	Motor Starter for Valve 26F	Does Not Close
JCB0073N	Motor Starter for Valve 73	Does Not Close
JCB0025N	Motor Starter for Valve 25	Does Not Close
JMV0257N	Pump Recirculation Valve 257	Does Not Close
JCB0257N	Motor Starter for Valve 257	Does Not Close
JMV0053N	Pump Recirculation Valve 53	Does Not Close
JCB0053N	Pump Recirculation Valve 53	Does Not Close
JCV0043P	Check Valve 43	Does Not Open
JCV0161P	Check Valve 161	Does Not Open

BEST DOCUMENT AVAILABLE


HPI
SINGLE FAULTS
JTKDHTIR
JTKDHTIX
JTKDHTIE
JPP0001R
SEE NOTE 1
JMV0257N
JCB0257N
JMV0053N
JCB0053N
DOUBLE FAULTS
TRAIN A FAULTS
TESFASAW
K480V3A1
E125DCAW
JMV0073P
K4160V3A
BNUSWCCW
JCV0072P
JCB0073N
JRVDH69P
SEE NOTE 2
TRAIN B FAULTS
TESFASBW
K480V3B1
E125DCBW
JMV0058Q
K4160V3B
BDHTCCCW
JCV0060P
JRVDH70P
JXV0059X
JCV0002X
JCV0001P
JPM001CR
JCB001CN
SEE NOTE 2
K480V3A1
JSWXFERX
TWO OF THREE FAULTS
2/3
INJECTION LINE 3A1 FAULTS
JCV0043P
JCV0161P
JMV024FP
JCB024FN
INJECTION LINE 3A2 FAULTS
JCV0042P
JCV0160P
JMV023FP
JCB023FN
COM
CAUSE
HARDWARE
ESFASAB

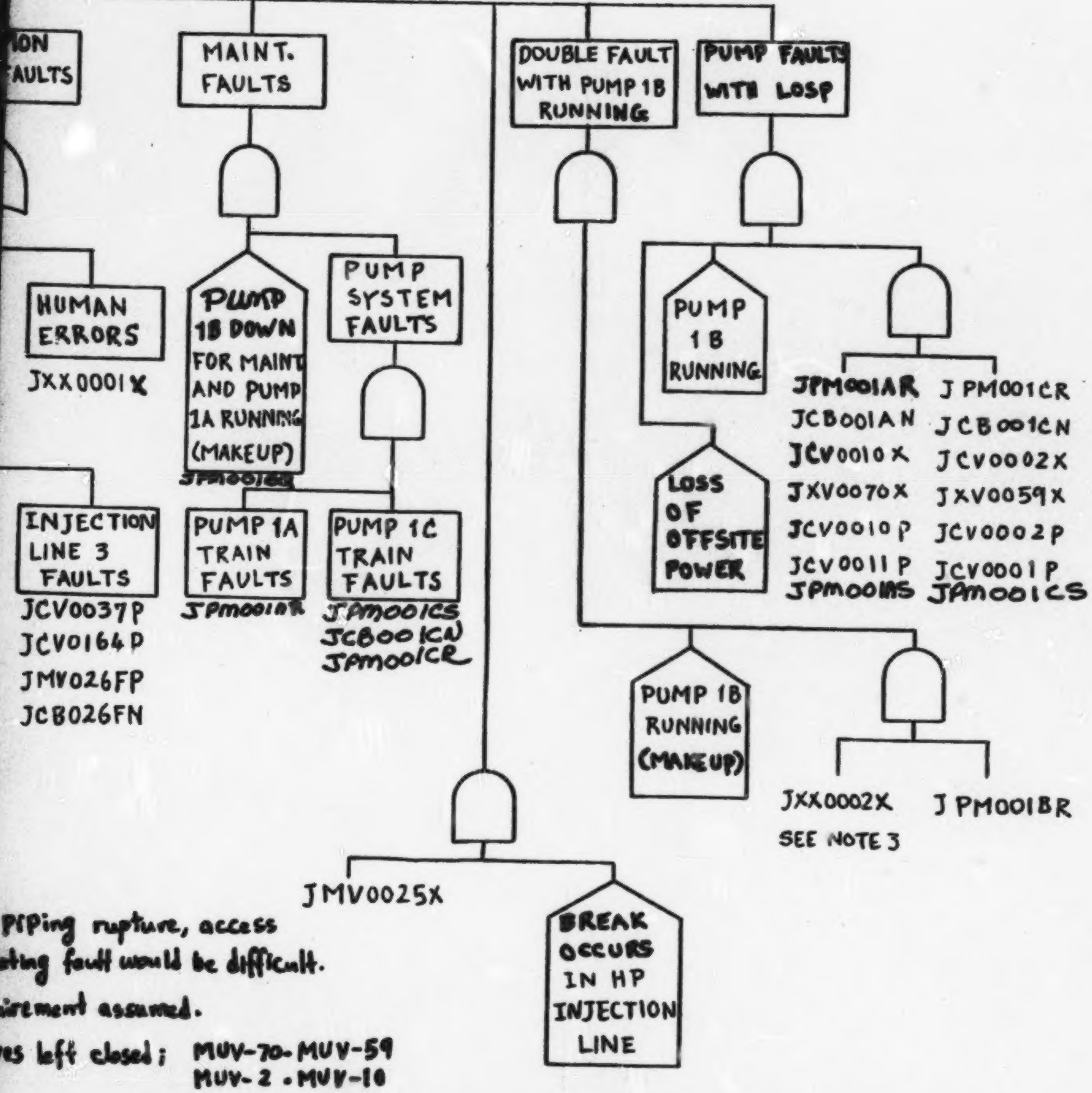
NOTES:

1. In the event of pum
to manual valves for is

2. Automatic start re

3. Any combination of v

BEST DOCUMENT AVAILABLE


ION
FAULTS
MAINT. FAULTS
DOUBLE FAULT WITH PUMP 1B RUNNING
PUMP FAULTS WITH LOSP
HUMAN ERRORS
JXX0001X
PUMP 1B DOWN FOR MAINT AND PUMP 1A RUNNING (MAKEUP)
JPM001BR
PUMP SYSTEM FAULTS
PUMP 1B RUNNING
JPM001AR
JCB001AN
JCV0010X
JXV0070X
JCV0010P
JCV0011P
JPM001AS
JPM001CR
JCB001CN
JCV0002X
JXV0059X
JCV0002P
JCV0001P
JPM001CS
LOSS OF OFFSITE POWER
INJECTION LINE 3 FAULTS
JCV0037P
JCV0164P
JMV026FP
JCB026FN
PUMP 1A TRAIN FAULTS
JPM001AR
PUMP 1C TRAIN FAULTS
JPM001CS
JCB001CN
JPM001CR
PUMP 1B RUNNING (MAKEUP)
JXX0002X
SEE NOTE 3
JPM001BR
JMV0025X
BREAK OCCURS IN HP INJECTION LINE

, Piping rupture, access
olating fault would be difficult.

quirement assumed.

lves left closed; MUV-70 · MUV-59
MUV-2 · MUV-10
MUV-2 · MUV-70
MUV-10 · MUV-59

Figure G.2 Simplified Fault Tree - High Pressure System (For Fault Summary see Table G.1)

G.3 SYSTEM QUANTIFICATION

G.3.1 SYSTEM RELIABILITY CHARACTERISTICS

The Crystal River HPI system is basically a two pump train system but with the following characteristics that affect the reliability of the system:

- Pump Train A employs two parallel pumps (MUP-1B, MUP-1A), while pump Train B employs a single pump (MUP-1C). One pump on pump Train A is normally operating.
- There is a crossover at the discharge side of the pumps, so that any pump can pump into any of four discharge lines. (Two out of three lines other than the break line are required for success.)
- Components are maintained only after they fail. The only maintenance contribution assessed was that due to failure of MUP-1B.
- Pump and valve testing were assumed not to alter the system unavailability.

System interfaces include AC power, DC power, and component cooling. The NSCCCS provides component cooling for the Train A pumps, while the Train B pump is cooled by the DHCCCS. Train A equipment interfaces with AC power and DC power Train A, while Train B equipment interfaces with AC and DC power Train B.

For the case where off-site power is available, the dominant contributors to HPI system unavailability are operator error. Hardware and other contributions are about an order of magnitude lower than the operator error.

For the loss of offsite power case, various hardware faults (including diesel faults) are of the same order of magnitude as operator error. The system unavailability in this case is about a factor of two higher than in the case where offsite power is available. No one hardware contributor stands out as being dominant; but the aggregate increases the system unavailability by a factor of two.

A separate fault tree was constructed for the case where the HPI is used in the "Feed and Bleed" mode. For this case the dominant failure mode is that the operator will fail to establish feed and bleed, which is about two orders of magnitude higher than the aggregate hardware related faults.

G.3.2 SYSTEM FAULT TREE QUANTIFICATION - INJECTION PHASE

This section presents the quantification of the HPI unavailability for required emergency operation during the injection phase of a postulated accident or transient. The quantitative results are presented in table form with attached notes outlining the assumptions. Modularized fault trees were constructed from the simplified fault tree presented in Section G.2 as an aid to performing the quantification and sensitivity analyses.

Table G.2 shows the HPI success requirements for various transients and LOCA sizes, Table G.3 contains top event definitions for the modularized fault trees, and Figures G.3 through G.8 show the modularized fault trees. The unavailability of each gate is shown on these trees, as well as the unavailability of the top events. Table G.4 shows the Boolean equations that represent the fault trees. Table G.5, the HPI quantification table, shows the quantification of each gate by component and failure mode. The notes for this table explain the assumptions used in the quantification. Table G.6 summarizes the point estimates for each gate.

Table G.2 High Pressure Injection Success Requirements

INITIATOR	TRAINS	NOTES
B3, B4-LOCA	1/3 pump flow	1
	2/3 injection lines	2
Transient induced LOCA	1/3 pump flow	1
	2/3 injection	2
Transient with loss of all secondary cooling	1/3 pump flow	1
	2/4 injection lines	3

NOTES:
1. The HPI is a two-pump train system, where Train A consists of two parallel pumps (MUP-B, MUP-A) and Train B consists of a single pump (MUP-C)
2. The HPI contains four injection lines, but the injection line feeding into the leg containing the break is assumed to be ineffective for cooling the reactor.
3. All four injection lines are presumed potentially functional in this case.

Table G.3 High Pressure Injection - Top Events

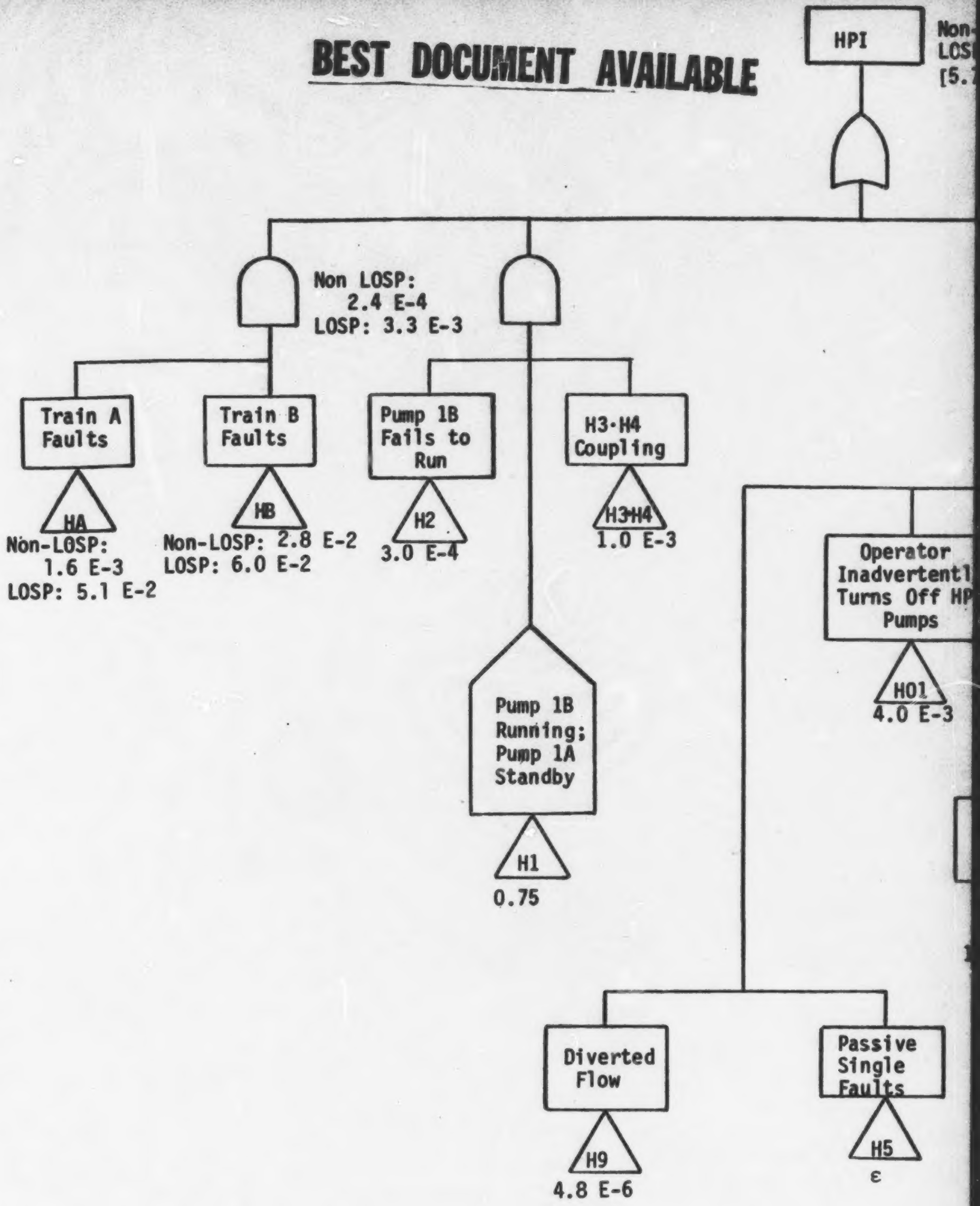
INITIATOR	BOOLEAN REPRESENTATION		
B4, B3-LOCAs; Transient induced LOCAs	HPI	High pressure injection system fails to provide one pump flow via two injection lines to cold legs	1
B4 LOCAs; Transient induced LOCAs.	HA	High pressure injection system Train A fails to provide one pump flow to injection line headers	1,2
	HB	High pressure injection system Train B fails to provide one pump flow to injection line headers	1,2
Transient with loss of all secondary cooling	HPFB	Operator fails to establish feed and bleed operation or high pressure injection system fails to provide one pump flow via two injection lines to cold legs	1
Transient with loss of all secondary cooling	HAF	High pressure injection Train A fails to provide one pump flow to injection line headers for feed and bleed	3
	HBF	High pressure injection Train B fails to provide one pump flow to injection line headers for feed and bleed	3

NOTES: 1. Requirements for break isolation or manual initiation are reflected in fault trees or Boolean equations for the individual initiators as appropriate.

2. HA and HB are required for modeling emergency coolant recirculation. Failure modes common to both trains are excluded from the individual train failures.

3. These events are defined for convenience of analysis, and correspond to events HA and HB, except that some failures in these events are not contained in HAF and HBF.

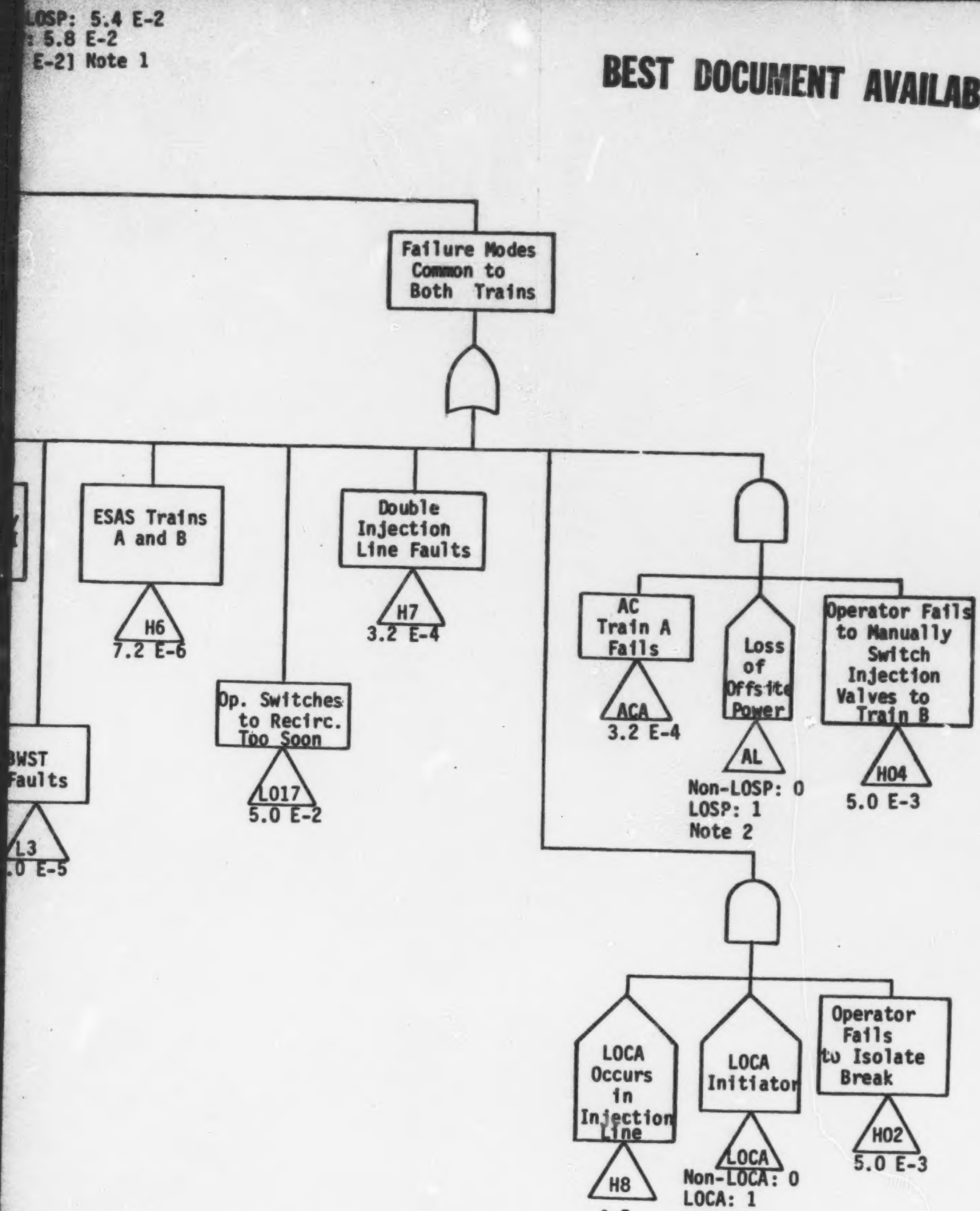
BEST DOCUMENT AVAILABLE


HPI
Non-
LOS
[5.7
Non LOSP:
2.4 E-4
LOSP: 3.3 E-3
Train A Faults
HA
Non-LOSP:
1.6 E-3
LOSP: 5.1 E-2
Train B Faults
HB
Non-LOSP: 2.8 E-2
LOSP: 6.0 E-2
Pump 1B Fails to Run
H2
3.0 E-4
H3·H4 Coupling
H3H4
1.0 E-3
Operator Inadvertentl Turns Off HP Pumps
HO1
4.0 E-3
Pump 1B Running; Pump 1A Standby
H1
0.75
Diverted Flow
H9
4.8 E-6
Passive Single Faults
H5
ε

Note 1: The unavailability in brackets is for the LOCA initiator

2: The initiating event for the tree is either a loss of offsite power or a LOCA, but not both simultaneously.

BEST DOCUMENT AVAILABLE


LOSP: 5.4 E-2
: 5.8 E-2
E-2] Note 1
Failure Modes Common to Both Trains
ESAS Trains A and B
H6
7.2 E-6
Double Injection Line Faults
H7
3.2 E-4
Op. Switches to Recirc. Too Soon
L017
5.0 E-2
BWST Faults
L3
.0 E-5
AC Train A Fails
ACA
3.2 E-4
Loss of Offsite Power
AL
Non-LOSP: 0
LOSP: 1
Note 2
Operator Fails to Manually Switch Injection Valves to Train B
H04
5.0 E-3
LOCA Occurs in Injection Line
H8
0.5
LOCA Initiator
LOCA
Non-LOCA: 0
LOCA: 1
Note 2
Operator Fails to Isolate Break
H02
5.0 E-3

259-A Figure G.3 Modularized Fault Tree for Event "HPI"

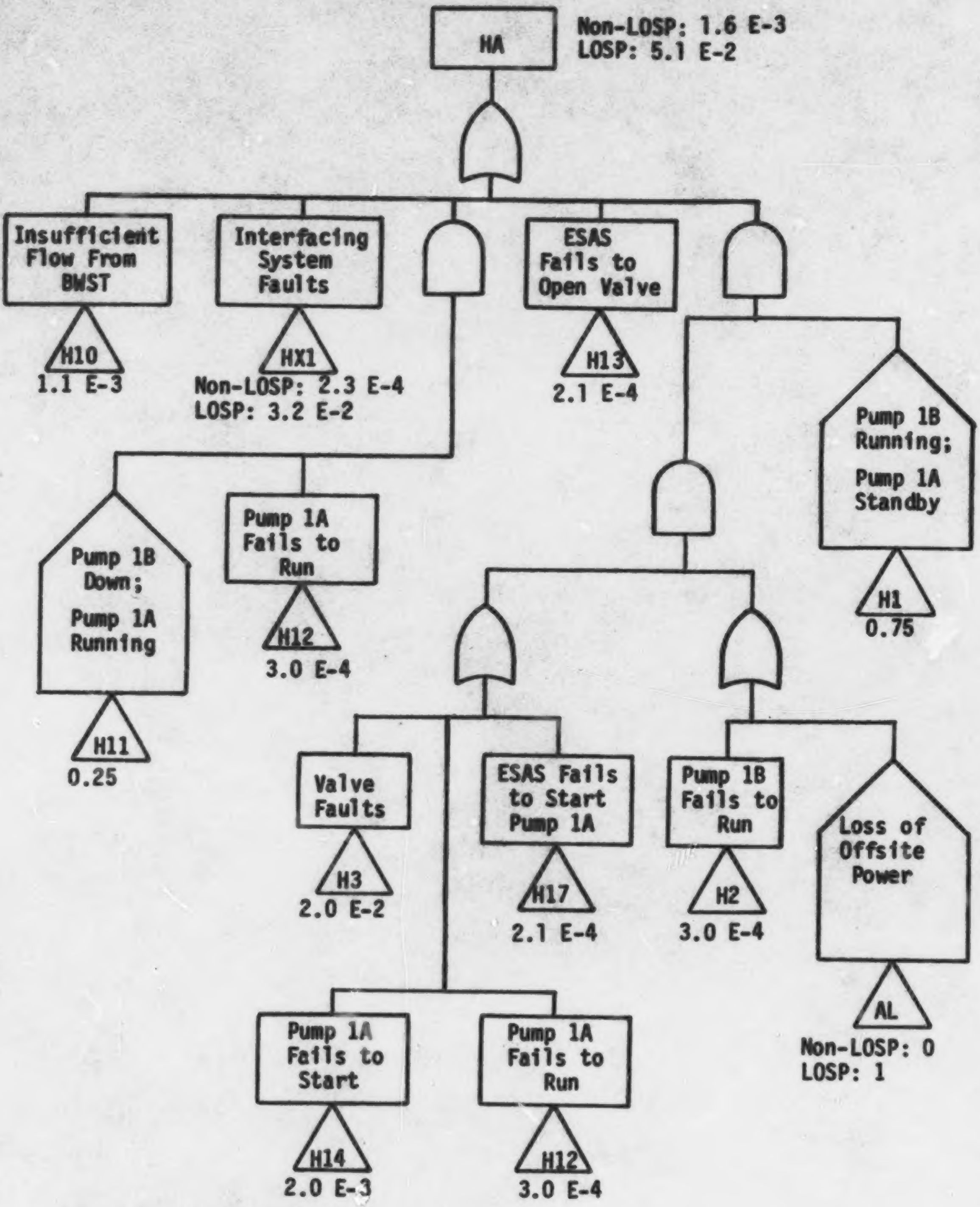

HA
Non-LOSP: 1.6 E-3
LOSP: 5.1 E-2
Insufficient Flow From BWST
H10
1.1 E-3
Interfacing System Faults
HX1
Non-LOSP: 2.3 E-4
LOSP: 3.2 E-2
ESAS Fails to Open Valve
H13
2.1 E-4
Pump 1B Running;
Pump 1A Standby
H1
0.75
Pump 1B Down;
Pump 1A Running
H11
0.25
Pump 1A Fails to Run
H12
3.0 E-4
Valve Faults
H3
2.0 E-2
ESAS Fails to Start Pump 1A
H17
2.1 E-4
Pump 1B Fails to Run
H2
3.0 E-4
Loss of Offsite Power
AL
Non-LOSP: 0
LOSP: 1
Pump 1A Fails to Start
H14
2.0 E-3
Pump 1A Fails to Run
H12
3.0 E-4

Figure G.4 Modularized Fault Tree for Event "HA"

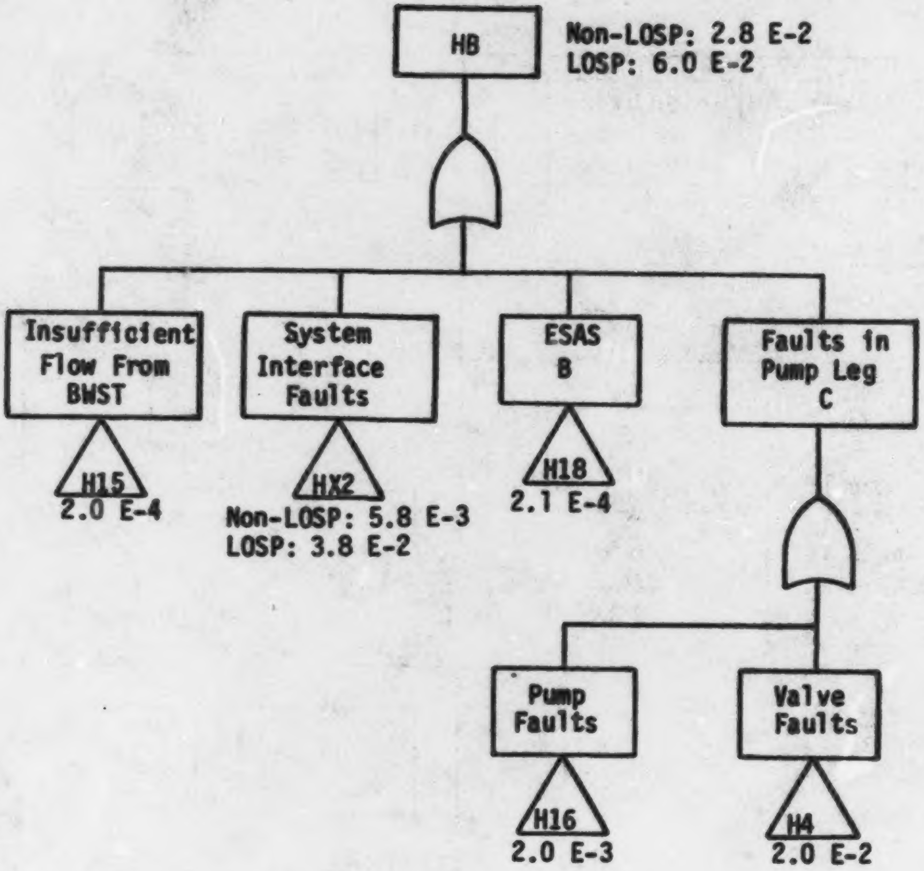

HB
Non-LOSP: 2.8 E-2
LOSP: 6.0 E-2
Insufficient Flow From BWST
H15
2.0 E-4
System Interface Faults
HX2
Non-LOSP: 5.8 E-3
LOSP: 3.8 E-2
ESAS B
H18
2.1 E-4
Faults in Pump Leg C
Pump Faults
H16
2.0 E-3
Valve Faults
H4
2.0 E-2

Figure G.5 Modularized Fault Tree for Event "HB"

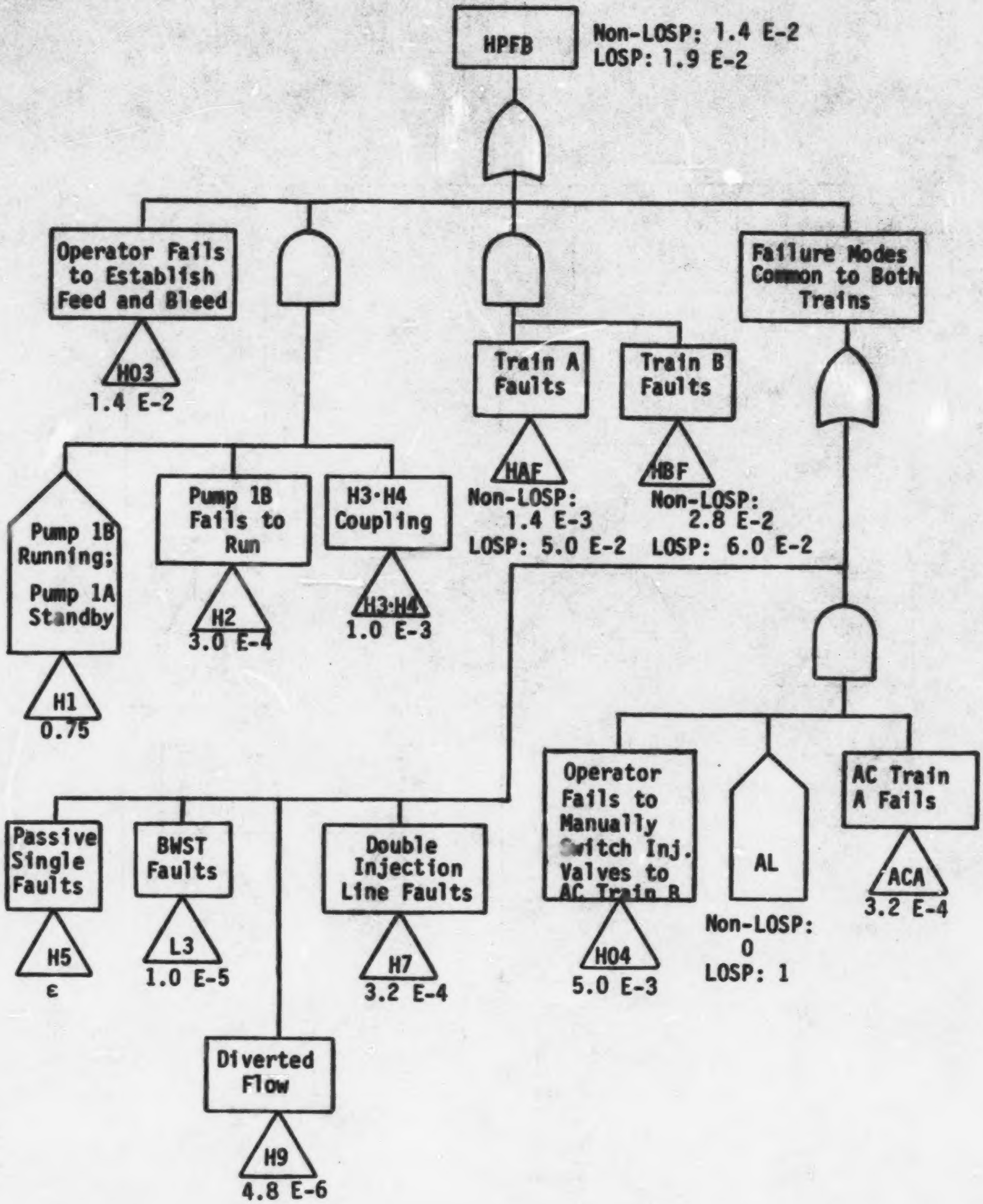

HPFB
Non-LOSP: 1.4 E-2
LOSP: 1.9 E-2
Operator Fails to Establish Feed and Bleed
HO3
1.4 E-2
Pump 1B Running; Pump 1A Standby
H1
0.75
Pump 1B Fails to Run
H2
3.0 E-4
H3·H4 Coupling
H3·H4
1.0 E-3
Train A Faults
HAF
Non-LOSP: 1.4 E-3
LOSP: 5.0 E-2
Train B Faults
HBF
Non-LOSP: 2.8 E-2
LOSP: 6.0 E-2
Failure Modes Common to Both Trains
Passive Single Faults
H5
ε
BWST Faults
L3
1.0 E-5
Double Injection Line Faults
H7
3.2 E-4
Diverted Flow
H9
4.8 E-6
Operator Fails to Manually Switch Inj. Valves to AC Train B
HO4
5.0 E-3
AL
Non-LOSP: 0
LOSP: 1
AC Train A Fails
ACA
3.2 E-4

Figure G.6 Modularized Fault Tree for Event "HPFB"

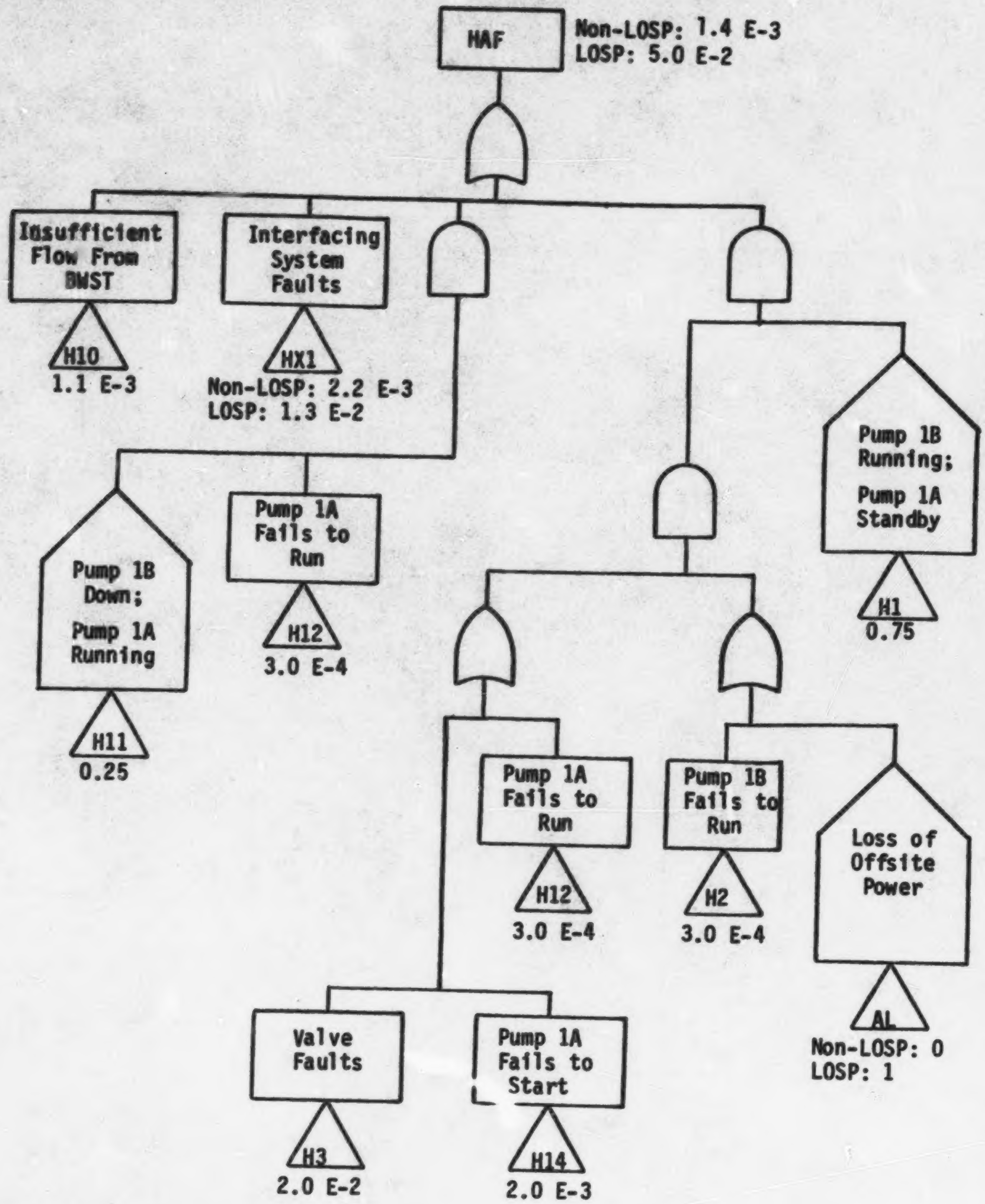

HAF
Non-LOSP: 1.4 E-3
LOSP: 5.0 E-2
Insufficient Flow From BWST
H10
1.1 E-3
Interfacing System Faults
HX1
Non-LOSP: 2.2 E-3
LOSP: 1.3 E-2
Pump 1B Down; Pump 1A Running
H11
0.25
Pump 1A Fails to Run
H12
3.0 E-4
Pump 1B Running; Pump 1A Standby
H1
0.75
Pump 1A Fails to Run
H12
3.0 E-4
Pump 1B Fails to Run
H2
3.0 E-4
Loss of Offsite Power
AL
Non-LOSP: 0
LOSP: 1
Valve Faults
H3
2.0 E-2
Pump 1A Fails to Start
H14
2.0 E-3

Figure G.7 Modularized Fault Tree for Event "HAF"

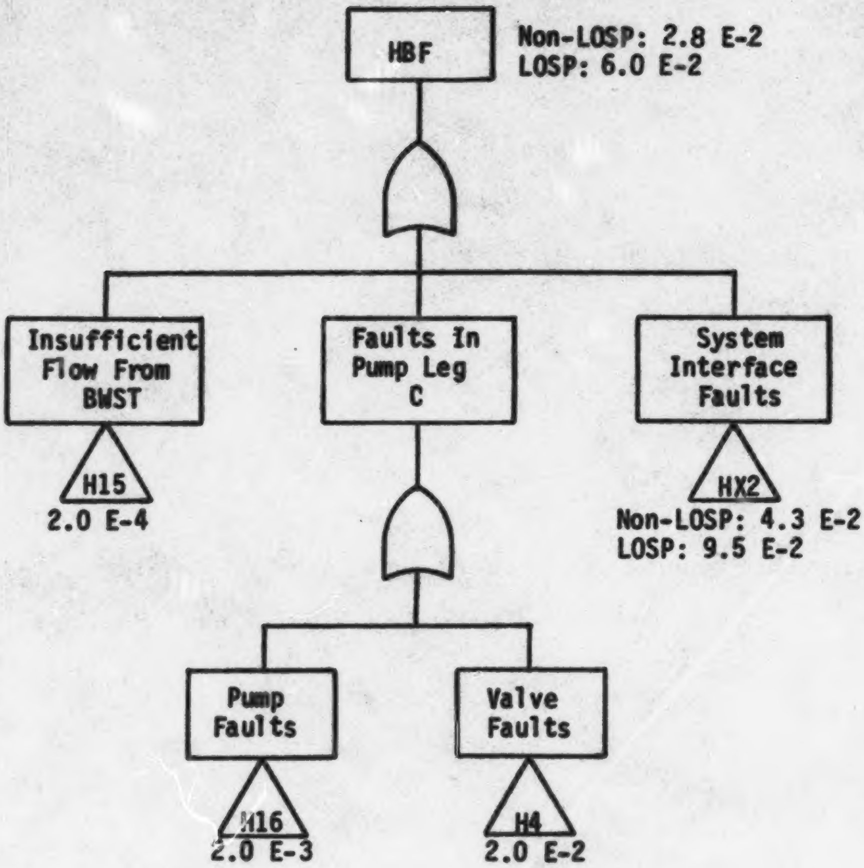

HBF
Non-LOSP: 2.8 E-2
LOSP: 6.0 E-2
Insufficient Flow From BWST
Faults In Pump Leg C
System Interface Faults
H15
2.0 E-4
HX2
Non-LOSP: 4.3 E-2
LOSP: 9.5 E-2
Pump Faults
Valve Faults
H16
2.0 E-3
H4
2.0 E-2

Figure G.8 Modularized Fault Tree for Event "HBF"

Table G.4 (1/2) HPI

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS

NOTES

$$\begin{aligned}
\mathrm{HPI} &= \mathrm{HA}\cdot\mathrm{HB} + \mathrm{H1}\cdot\mathrm{H2}\cdot(\mathrm{H3}\cdot\mathrm{H4}) + \mathrm{H5} + \mathrm{H6} + \mathrm{H7} + \mathrm{H9} + \mathrm{L3} + \\
&\quad + \mathrm{L017} + \mathrm{H01} + (\mathrm{H02}\cdot\mathrm{H8})\cdot\mathrm{LOCA} + (\mathrm{H04}\cdot\mathrm{ACA})\cdot\mathrm{AL} \\
\mathrm{HA} &= \mathrm{HX1} + \mathrm{H10} + \mathrm{H11}\cdot\mathrm{H12} + \mathrm{H13} + \mathrm{H1}\cdot(\mathrm{AL} + \mathrm{H2})\cdot(\mathrm{H3} + \mathrm{H12} + \mathrm{H17} + \mathrm{H14}) \\
\mathrm{HB} &= \mathrm{HX2} + \mathrm{H4} + \mathrm{H15} + \mathrm{H16} + \mathrm{H18}
\end{aligned}$$

INTERMEDIATE EVENTS

$$\begin{aligned}
\mathrm{HX1} &= \mathrm{ACA} + \mathrm{DCA} + \mathrm{N} && (1) \\
\mathrm{HX2} &= \mathrm{ACB} + \mathrm{DCB} + \mathrm{DB} && (1) \\
\mathrm{HX1}\bullet\mathrm{HX2} &= \mathrm{ACA}\bullet\mathrm{ACB} + \mathrm{ACA}\bullet(\mathrm{D2} + \mathrm{D4} + \mathrm{DM2} + \mathrm{DH2}) + \mathrm{DB}[\mathrm{N1} + \mathrm{N2}\ (\mathrm{N3} + \mathrm{NM2}) + \\
&\quad + \mathrm{N6}\bullet(\mathrm{N5} + \mathrm{NM4}) + \mathrm{N4}\bullet(\mathrm{N5} + \mathrm{N7} + \mathrm{NM4}) + \mathrm{NM3}\bullet(\mathrm{N5} + \mathrm{N7}) + \mathrm{N6}\bullet\mathrm{N7} + \\
&\quad + \mathrm{N3}\bullet\mathrm{NM1}] && (1)
\end{aligned}$$

BOOLEAN EQUATIONS REGROUPED FOR REDUCTION

TOP EVENT

$$\begin{aligned}
\mathrm{HPI} &= \mathrm{H5} + \mathrm{H6} + \mathrm{H7} + \mathrm{H9} + \mathrm{L3} + \mathrm{L017} + \mathrm{H01} + \mathrm{H02}\cdot\mathrm{H8}\cdot\mathrm{LOCA} + (\mathrm{H04}\cdot\mathrm{ACA})\cdot\mathrm{AL} + \\
&\quad + \mathrm{HX1}\cdot(\mathrm{H4} + \mathrm{H15} + \mathrm{H16} + \mathrm{H18}) + \mathrm{ACA}\bullet\mathrm{ACB} + \\
&\quad + \mathrm{HX2}\cdot\{\mathrm{H10} + \mathrm{H11}\cdot\mathrm{H12} + \mathrm{H13} + \mathrm{H1}\cdot[\mathrm{AL}\cdot(\mathrm{H3} + \mathrm{H12} + \mathrm{H17} + \mathrm{H14}) + \\
&\quad + \mathrm{H2}\cdot(\mathrm{H12} + \mathrm{H17} + \mathrm{H14}) + \mathrm{H2}\cdot\mathrm{H3}]\} + (\mathrm{H10} + \mathrm{H11}\cdot\mathrm{H12} + \mathrm{H13})\cdot \\
&\quad \cdot(\mathrm{H4} + \mathrm{H15} + \mathrm{H16} + \mathrm{H18}) + \mathrm{H1}\cdot\ \{(\mathrm{H4} + \mathrm{H15} + \mathrm{H16} + \mathrm{H18})\cdot \\
&\quad \cdot[\mathrm{AL}\cdot(\mathrm{H3} + \mathrm{H12} + \mathrm{H17} + \mathrm{H14}) + \mathrm{H2}(\mathrm{H12} + \mathrm{H17} + \mathrm{H14})] + \\
&\quad + \mathrm{H2}\cdot\mathrm{H3}\cdot(\mathrm{H15} + \mathrm{H16} + \mathrm{H18}) + \mathrm{H2}\cdot(\mathrm{H3}\cdot\mathrm{H4})\} + \\
&\quad + \mathrm{ACA}\bullet(\mathrm{D2} + \mathrm{D4} + \mathrm{DM2} + \mathrm{DH2}) + \mathrm{DB}\ [\mathrm{N1} + \mathrm{N2}\bullet(\mathrm{N3} + \mathrm{NM2}] + \\
&\quad + \mathrm{N6}\bullet(\mathrm{N5} + \mathrm{NM4}) + \mathrm{N4}\bullet(\mathrm{N5} + \mathrm{N7} + \mathrm{NM4}) + \mathrm{NM3}\bullet(\mathrm{N5} + \mathrm{N7}) + \mathrm{N6}\bullet\mathrm{N7} + \mathrm{N3}\bullet\mathrm{NM1}] && (1)
\end{aligned}$$

Table G.4 (2/2) HPI - Feed and Bleed

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENTS **NOTES**

$$HPFB = H5 + H7 + H9 + L3 + H03 + H04 \cdot ACA \cdot AL + H1 \cdot H2 \cdot (H3 \cdot H4) + HAF \cdot HBF$$

$$HAF = H10 + H11 \cdot H12 + HX1 + H1 \cdot (AL + H2) \cdot (H3 + H12 + H14)$$

$$HBF = H4 + H15 + H16 + HX2$$

INTERMEDIATE EVENTS

$$HX1 = ACA + DCA + N \qquad (1)$$

$$HX2 = ACB + DCB + DB \qquad (1)$$

$$\begin{aligned} HX1 \cdot HX2 = {} & ACA \cdot ACB + ACA \cdot (D2 + D4 + DM2 + DH2) + DB \Big[N1 + N2 \cdot (N3 + NM2) + \\ & + N6 \cdot (N5 + NM4) + N4 \cdot (N5 + N7 + NM4) + NM3 \cdot (N5 + N7) + N6 \cdot N7 + \\ & + N3 \cdot NM1 \Big] \qquad (1) \end{aligned}$$

BOOLEAN EQUATIONS REGROUPED FOR REDUCTION

TOP EVENT

$$\begin{aligned} HPFB = {} & H5 + H7 + H9 + L3 + H03 + H04 \cdot ACA \cdot AL + HX1 \cdot (H4 + H15 + H16) + \\ & + ACA \cdot ACB + HX2 \cdot [H10 + H11 \cdot H12 + H1 \cdot (H2 + AL) \cdot (H3 + H12 + H14)] + \\ & + (H10 + H11 \cdot H12) \cdot (H4 + H15 + H16) + H1 \cdot (H2 + AL) \cdot [(H15 + H16) \cdot \\ & \cdot (H3 + H12 + H14) + H4 \cdot (H12 + H14) + (H3 \cdot H4)] + \\ & + ACA \cdot (D2 + D4 + DM2 + DH2) + DB \Big[N1 + N2 \cdot (N3 + NM2) + \\ & + N6 \cdot (N5 + NM4) + N4 \cdot (N5 + N7 + NM4) + NM3 \cdot (N5 + N7) + N6 \cdot N7 + \\ & + N3 \cdot NM1 \Big] \qquad (1) \end{aligned}$$

NOTES: (1) See appropriate system fault tree section for definition of faults whose initial letters are D (DHCCCS) or N (NSCCCS).

BEST DOCUMENT AVAILABLE

Table G.5 (1/5) Events "HA" and "HB" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
H10		INSUFFICIENT FLOW FROM BWST TO TRAIN A PUMPS			1.1 E-3			
	VALVE MUV-73	N.C. VALVE FAILS TO OPEN	D		1.0 E-3	$3^+, 3^-$		
	CHECK VALVE 72	PLUGGED	D		1.0 E-4			
					Σ=1.1 E-3			
H3		TRAIN A VALVE FAULTS			2.0 E-2	$3^+, 10^-$		
	MANUAL VALVE 70	LEFT CLOSED	D		1.0 E-2	$3^+, 10^-$	H	
	STOP CHECK VALVE 10	LEFT CLOSED	D		1.0 E-2	$3^+, 10^-$	H	
	CHECK VALVE 11	PLUGGED	D		1.0 E-4	$3^+, 3^-$		
					Σ=2.0 E-2			
H14		TRAIN A PUMP FAULTS			2.0 E-3			
	PUMP MUP-1A	FAILS TO START	D		1.0 E-3	$3^+, 3^-$		
	CIRCUIT BKR.	FAILS TO CLOSE	D		1.0 E-3	$3^+, 3^-$		
					Σ=2.0 E-3			
H12	PUMP MUP-1A	PUMP 1A FAILS TO RUN, GIVEN RUNNING AT ONSET OF INCIDENT	3.0 E-5	10	3.0 E-4	$10^+, 10^-$		1
H2	PUMP MUP-1B	PUMP-1B FAILS TO RUN, GIVEN RUNNING AT ONSET OF INCIDENT	3.0 E-5	10	3.0 E-4	$10^+, 10^-$		1
H15		INSUFFICIENT FLOW FROM BWST TO TRAIN B PUMP			2.0 E-4			
	VALVE MUV-58	N.O. VALVE FAILED CLOSED	D		1.0 E-4	$3^+, 3^-$		
	CHECK VALVE 60	PLUGGED	D		1.0 E-4	$3^+, 3^-$		
					Σ=2.0 E-4			
H4		TRAIN B VALVE FAULTS			2.0 E-2	$3^+, 10^-$	H	
	MANUAL VALVE 59	LEFT CLOSED	D		1.0 E-2	$3^+, 10^-$	H	
	STOP CHECK VALVE 2	LEFT CLOSED	D		1.0 E-2	$3^+, 10^-$	H	
	CHECK VALVE 1	PLUGGED	D		1.0 E-4	$3^+, 3^-$		
					Σ=2.0 E-2			

Table G.5 (2/5) Events "HA", "HB", and "HPI" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
H16		TRAIN B PUMP FAULTS			2.0 E-3			
	PUMP MUP-1C	FAILS TO START	D		1.0 E-3	$3^+, 3^-$		
	CIRCUIT BKR.	FAILS TO CLOSE	D		1.0 E-3	$3^+, 3^-$		
					Σ =2.0 E-3			
H1		PUMP 1B RUNNING, PUMP 1A ON STANDBY AT ONSET OF INCIDENT			.75			2
H11		PUMP 1B DOWN, PUMP 1A RUNNING AT ONSET OF INCIDENT			.25			2
AL		INITIATOR IS LOSS OF OFFSITE POWER			1 OR 0			3
H5		PASSIVE SINGLE FAULTS COMMON TO BOTH TRAINS			ϵ			
L3		SINGLE BWST FAILURES	D		1.0 E-5	$2^+, 2^-$	B	4, 5
H8·H02		OPERATOR FAILS TO ISOLATE BREAK IN INJECTION LINE			2.5 E-3	$3^+, 10^-$	0	
H8	INJECTION LINE	BREAK OCCURS IN INJECTION LINE, GIVEN THAT SMALL-SMALL BREAK OCCURS			0.5			6
H02	INJECTION LINE	OPERATOR FAILS TO CLOSE VALVE	D		5.0 E-3	$3^+, 10^-$	0	
					π = 2.5 E-3			
H3·H4	MANUAL VALVES 10, 70, 2, 59	2 VALVES LEFT CLOSED IN ANY OF THE COMBINATIONS: 70-59, 2-10, 70-2, 10-59	D		1.0 E-3	$10^+, 10^-$	H	7
LOCA		LOCA GATE						
		LOCA			1			
		NON LOCA			0			
H01	OPERATOR	OPERATOR INCORRECTLY TURNS OFF PUMPS AND FAILS TO RECOVER IN TIME TO MITIGATE INCIDENT	D		4.0 E-3	$10^+, 3^-$	0	8,17

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table G.5 (3/5) Events "HPI" and "HPFB" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
L017	OPERATOR	OPERATOR RECONFIGURES VALVES FOR RECIRCULATION TOO SOON AND LOSES SUCTION TO PUMPS	D		5.0 F 2	$3^+, 10^-$	0	9,17
H9		DIVERSION OF FLOW VIA FAILURE TO CLOSE MVs 257 AND 53			4.8 E-6			10
	MV 257	FAILS TO CLOSE	D		1.0 E-3	$3^+, 3^-$		
	CIRCUIT BKR 257	FAILS TO CLOSE	D		1.0 E-3	$3^+, 3^-$		
	ESAS/MV 257	NO ESAS SIGNAL TO CLOSE VALVE (ISSI)	D		2.1 E-4	$3^+, 3^-$		11
					Σ=2.2 E-3			
	MV 53	FAILS TO CLOSE	D		1.0 E-3	$3^+, 3^-$		
	CIRCUIT BKR 257	FAILS TO CLOSE	D		1.0 E-3	$3^+, 3^-$		
	ESAS/MV 53	NO ESAS SIGNAL TO CLOSE VALVE (ISSI)	D		2.1 E-4			11
					Σ=2.2 E-3			
H03		OPERATOR FAILS TO ESTABLISH FEED AND BLEED OPERATION	D		1. E-2	$3^+, 10^-$	0	12, 17
ACA·H04		INSUFFICIENT AC POWER ON TRAIN A AND OPERATOR FAILS TO SWITCH INJECTION VALVES 23F AND 24F TO TRAIN B			3.2 E-4	$3^+, 10^-$	0	13
ACA		AC POWER TRAIN A						
		INSUFFICIENT POWER (LOSP)			3.2 E-2			13
H04	OPERATOR	FAILS TO TRANSFER SWITCH	D		5.0 E-3	$3^+, 10^-$	0	
					Π=3.2 E-4			
H7		DOUBLE INJECTION LINE FAULTS			3.2 E-4			
	VALVE FAULTS	VALVE FAILURE IN 2 INJECTION LINES (FAILURE OF ANY 2 OF 3 INJECTION LINES			3.2 E-4	$2^+, 2^-$	B	15, 16
		INJECTION LINE A1 FAILURE						
	MV24F	FAILS TO OPEN	D		1.0 E-3	$3^+, 3^-$		
	CIRCUIT BKR. 24F	FAILS TO CLOSE	D		1.0 E-3	$3^+, 3^-$		
	CHECK VALVE 43	FAILS TO OPEN	D		1.0 E-4	$3^+, 3^-$		

Table G.5 (4/5) Events "HPFB", "HAF", "HBF", and "HPI" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
	CHECK VALVE 161	FAILS TO OPEN	D		1.0 E-4	3^+, 3^-		
	ESAS/MV 24F	NO ESAS SIGNAL TO OPEN VALVE (ISSI)	D		2.1 E-4			11
					Σ= 2.4 E-3			
		INJECTION LINE A2 FAILURE						
	MV 23F	FAILS TO OPEN	D		1.0 E-3			
	CIRCUIT BKR. 23F	FAILS TO CLOSE	D		1.0 E-3			
	CHECK VALVE 42	FAILS TO OPEN	D		1.0 E-4			
	CHECK VALVE 160	FAILS TO OPEN	D		1.0 E-4			
	ESAS/MV 23F	NO ESAS SIGNAL TO OPEN VALVE (ISSI)	D		2.1 E-4			11
					Σ= 2.4 E-3			
		INJECTION LINE B2 FAILURE						
	MV 26F	FAILS TO OPEN	D		1.0 E-3			
	CIRCUIT BKR. 26F	FAILS TO CLOSE	D		1.0 E-3			
	CHECK VALVE 37	FAILS TO OPEN	D		1.0 E-4			
	CHECK VALVE 164	FAILS TO OPEN	D		1.0 E-4			
	ESAS/MV 26F	NO ESAS SIGNAL TO OPEN VALVE (ISSI)	D		2.1 E-4			11
					Σ= 2.4 E-3			
	MVs 23F, 24F, AND 26F	COUPLED FAILURE TO OPEN OF ANY 2 VALVES			3.0 E-4	2^+, 2^-		14
H17	ESAS/MUP-1A	NO ESAS SIGNAL TO START PUMP (ISSI)			2.1 E-4			11
H13	ESAS/MUV-73	NO ESAS SIGNAL TO OPEN VALVE (ISSI)			2.1 E-4			11
H18	ESAS/MUP-1C	NO ESAS SIGNAL TO START PUMP (ISSI)			2.1 E-4			11
H6		NO SIGNALS FROM ESAS-A AND ESAS-B AND FAILURE TO RECOVER	(7.2 E-4)(0.01)		7.2 E-6			11
ACA		INSUFFICIENT AC POWER - TRAIN A						
		WITH LOSS OF OFFSITE POWER			3.2 E-2			
		FOR OTHER INITIATORS						

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table G.5 (5/5) Events "HPI" and "HPFB" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR-1)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
ACB		INSUFFICIENT AC POWER - TRAIN B						
		WITH LOSS OF OFFSITE POWER			3.2 E-2			
		FOR OTHER INITIATORS			ε			
ACA·ACB		INSUFFICIENT AC POWER ON BOTH TRAINS						
		WITH LOSS OF OFFSITE POWER			2.3 E-3			
		FOR OTHER INITIATORS			ε			
DCA		INSUFFICIENT DC POWER - TRAIN A						
		NON LOSP			ε			
		LOSP			3.2 E-3			
DCB		INSUFFICIENT DC POWER - TRAIN B						
		NON LOSP			ε			
		LOSP			3.2 E-3			
N		NSCCCS FAILURE						
		NON LOSP			1.3 E-4			11
		LOSP			2.8 E-3			
DB		DHCCCS - TRAIN B FAILURE						
		NON LOSP			5.8 E-3			11
		LOSP			3.8 E-2			
		NSCCCS TRAIN B FAULTS						11, 18
		NSCCCS TRAIN A FAULTS						11, 18
		NSCCCS DOUBLE FAULTS						11, 18
		DHCCCS TRAIN B FAULTS						11, 18

Table G.5 (1/2) Quantification - HPI

NOTES: 1. The 10 hour operation timed assumed for the injection phase is conservative for those small breaks which do not require draws on the BWST by other systems.

2. Pump 1B is assumed to be out of service for 3 months per year. Technical Specifications do not limit the outage time.

3. The house is 1 for Loss of Offsite Power transients, 0 for all other initiators.

4. The BWST water level is monitored continuously and alarmed in the control room.

5. See Table K.6.

6. The probability of 0.5. is assumed and applied to LOCA initiators only. An opportunity for this fault would occur at each ESAS signal.

7. This fault represents a coupled human act. The probability that any one valve would be closed is estimated to be 1E-2. The probability that any one of the four combinations of two valves would be closed, given that one valve was closed, is estimated to be 0.1.

8. This fault occurred at TMI. Because of new NRC regulations and increased operator awareness, the likelihood of this fault is assumed to be less now than prior to TMI.

9. Reconfiguration for recirculation of both the high and low pressure ECCS and the reactor building spray system is considered to be a single act. Hence, the fault L017 also appears in the fault trees for the other systems.

10. Gate H9 represents double failure of the two sub-gates shown.

11. See appropriate system fault tree analysis section.

12. The probability is estimated to be relatively high because (1) the operator would likely be reluctant to carry out the procedure, since in effect it requires that he create a LOCA; the ramifications of doing it unnecessarily would be serious, and (2) the procedure is relatively complex in that it involves numerous actions.

Table G.5 (2/2) Quantification - HPI

NOTES: 13. The unavailability shown for ACA is for the loss of Offsite Power transient. The unavailability for ACA, and therefore the contribution of the double fault ACA·H04, is negligible in the case of other initiators.

14. The probability of failure of two valves is (1E-3)(0.1) = 1E-4, where 0.1 is the coupling probability assumed. There are three pairs of valves, hence the total fault probability is 3(1E-4) = 3E-4. (See also note 16.)

15. The probability estimate for H7 is comprised of contributions for both "independent" failures and coupled failures. The independent failure contribution is estimated as 3(2.4 E-3)·(2.4 E-3) = 1.7 E-5, where 2.4 E-3 is the failure probability of a single injection line as tabulated. The coupling contribution 3.0E-4 is listed separately.

16. No credit is taken for flow through the injection line affected by the initiator.

17. This human error was evaluated using THERP tree analysis as described in NUREG/CR-1278.

18. Faults from this system contribute to system interface faults HX1 and HX2. See Boolean equations for HPI system faults for identification of the contributing faults.

Table G.6 (1/2) HPI, HPFB - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
H10	1.1 E-3
H3	2.0 E-2
H14	2.0 E-3
H12	3.0 E-4
H2	3.0 E-4
H15	2.0 E-4
H4	2.0 E-2
H16	2.0 E-3
H1	0.75
H11	0.25
AL	0* 1**
H5	ε
L3	1.0 E-5
H8·H02	2.5 E-3
H8	0.5
H02	5.0 E-3
H3·H4	1.0 E-3
LOCA	0+ 1++
H7	3.2 E-4
ACA·H04	3.2 E-4
ACA	3.2 E-2
H04	5.0 E-3

*Offsite power available

**Offsite power not available

+non LOCA

++LOCA

Table G.6 (2/2) HPI, HPFB - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
H01	4.0 E-3
L017	5.0 E-2
H9	4.9 E-6
H03	1.4 E-2
H17	2.1 E-4
H13	2.1 E-4
H18	2.1 E-4
H6	7.2 E-6
ACA	3.2 E-2
ACB	3.2 E-2
ACA·ACB	2.3 E-3
DCA	ε* 3.2 E-3**
DCB	ε* 3.2 E-3**
N	1.3 E-4* 2.8 E-3**
DB	5.9 E-3* 3.8 E-2**

*Offsite power available
**Offsite power not available

G.3.3 SYSTEM FAULT TREE QUANTIFICATION - RECIRCULATION PHASE

This section presents the quantification of the High Pressure System unavailability for required emergency operation during the recirculation phase of a postulated accident or transient. The quantitative results are presented in table form with attached notes outlining the assumptions. A modularized fault tree was constructed as an aid in performing the quantification and sensitivity analysis.

Table G.7 shows the HPR success requirements for various transients and LOCA sizes, Table G.8 contains top event definitions for the modularized fault trees, and Figures G.9 and G.10 show the modularized fault trees. The unavailability of each gate is shown on this tree, as well as the unavailability of the top event. Table G.9 shows the Boolean equation that represents this fault tree. Table G.10, the HPR quantification table, shows the quantification of each gate by component and failure mode. The notes for this table explain the assumptions used in the quantification. Table G.11 summarizes the point estimates for each gate.

Table G.7 High Pressure Recirculation - Success Requirements

INITIATOR	TRAINS	NOTES
B4 LOCA	1/2	1,2,3,4
Transient induced LOCA	1/2	1,2,3,4
Transient with loss of all secondary cooling	1/2	5

NOTES:
1. The event tree structure presumes that high pressure recirculation fails if high pressure injection fails. The high pressure recirculation fault tree analysis is therefore predicated on success of the injection phase.
2. Single train failures in the injection phase are assumed not to be recovered for the recirculation phase (with one exception as indicated in Note 3). This assumption is somewhat conservative in that there may be some chance of recovery for some faults, such as manual valves left in the wrong position; however, even if credit for recovery were given, it would make very little difference in the quantification of HPR.
3. For loss of offsite power transients, single train failures due to failure of a diesel generator are assumed to be recoverable for recirculation, since there is a high probability that offsite power would be recovered (within 5-10 hours).
4. The recirculation phase analysis is based on an operating period of 24 hours following the initiating event.
5. If the "feed and bleed" operation extends into the recirculation phase, one of two trains would be required for success. However, injection failure would be the most likely cause of failure to provide makeup; primarily because of the possibility of operator faults. For this reason, high pressure recirculation was not evaluated for this set of transients.

Table G.8 High Pressure Recirculation - Top Events

BOOLEAN REPRESENTATION	TOP EVENT	NOTES
HPR	High pressure system fails to provide at least one pump flow via two injection lines to cold legs in the recirculation phase, given HPI succeeds and the corresponding low pressure trains provide adequate suction head to the high pressure pumps.	
HA*	High pressure system Train A fails to provide at least one pump flow to injection line headers during recirculation, given success during injection and adequate suction head from the corresponding low pressure pump.	1
HB*	High pressure system Train B fails to provide one pump flow to injection line headers during recirculation, given success during injection and adequate suction head from the corresponding low pressure pump.	1

NOTES: 1. For loss of offsite power transients, injection failures due to diesel failures are assumed to be recovered for recirculation. For events HA* and HB*, diesel failures therefore do not preclude "success during injection" as specified in the top event definitions.

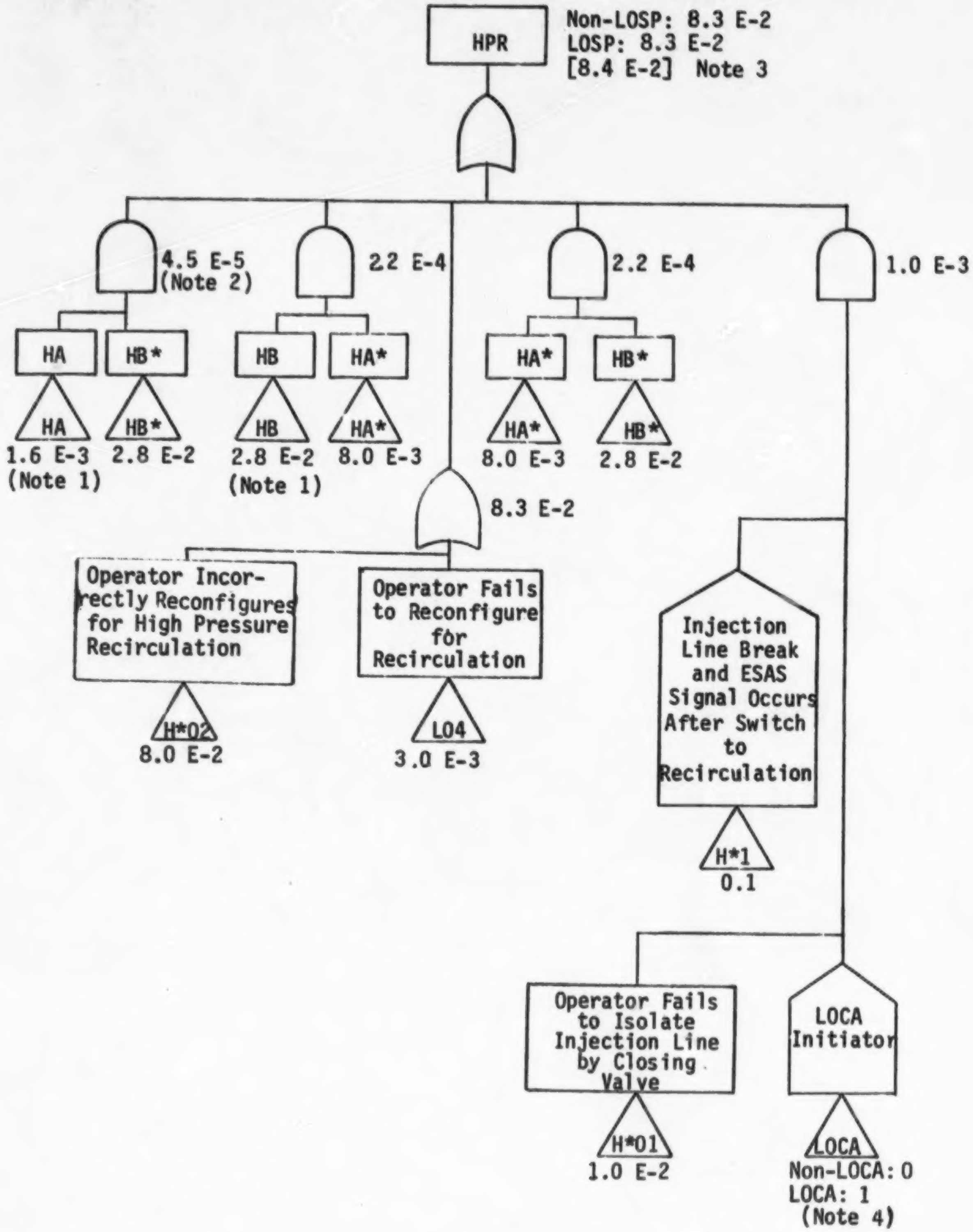

HPR
Non-LOSP: 8.3 E-2
LOSP: 8.3 E-2
[8.4 E-2] Note 3
4.5 E-5
(Note 2)
2.2 E-4
2.2 E-4
1.0 E-3
HA
HB*
HB
HA*
HA*
HB*
HA
HB*
HB
HA*
HA*
HB*
1.6 E-3
(Note 1)
2.8 E-2
2.8 E-2
(Note 1)
8.0 E-3
8.0 E-3
2.8 E-2
8.3 E-2
Operator Incorrectly Reconfigures for High Pressure Recirculation
H*02
8.0 E-2
Operator Fails to Reconfigure for Recirculation
L04
3.0 E-3
Injection Line Break and ESAS Signal Occurs After Switch to Recirculation
H*1
0.1
Operator Fails to Isolate Injection Line by Closing Valve
H*01
1.0 E-2
LOCA Initiator
LOCA
Non-LOCA: 0
LOCA: 1
(Note 4)

Figure G.9 Modularized Fault Tree Event "HPR"

Figure G.9 HPR Modularized Fault Tree

NOTES:

1. For sequences involving loss of offsite power, offsite power is assumed to be recovered by the recirculation phase, therefore "Non-LOSP" values are used in HPR for HA and HB in all cases. (The injection phase is assumed to last about 10 hours for the B_4 LOCA.) This means that diesel failures do not contribute to system failure in the recirculation phase.
2. See HPI fault tree quantification tables for HA and HB.
3. The number in brackets is for the LOCA initiator.
4. The initiating event assumed for the tree is either a loss of offsite power or a LOCA, but not both simultaneously. A transient induced LOCA is treated as a transient event.

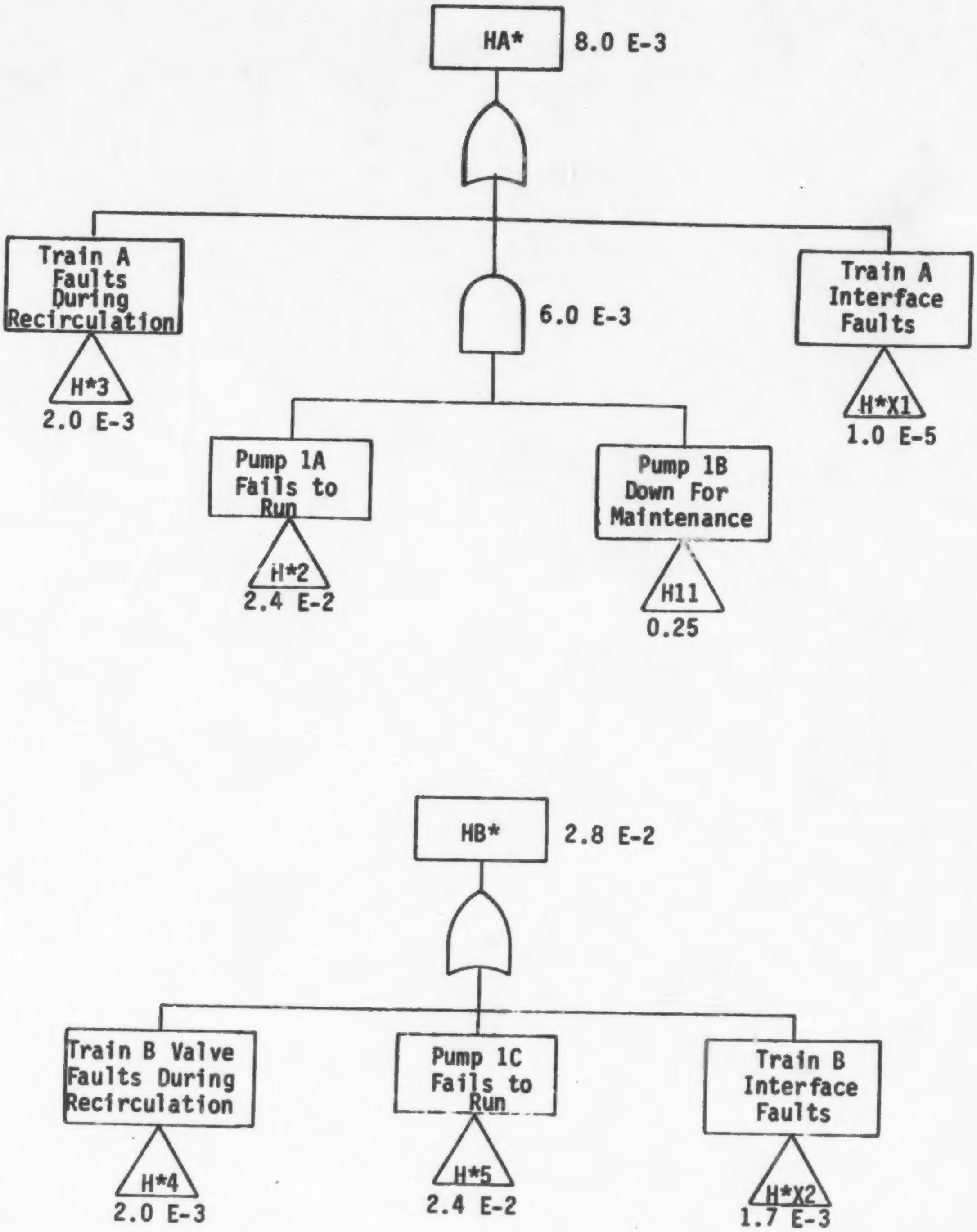

HA*
8.0 E-3
Train A Faults During Recirculation
H*3
2.0 E-3
6.0 E-3
Train A Interface Faults
H*X1
1.0 E-5
Pump 1A Fails to Run
H*2
2.4 E-2
Pump 1B Down For Maintenance
H11
0.25
HB*
2.8 E-2
Train B Valve Faults During Recirculation
H*4
2.0 E-3
Pump 1C Fails to Run
H*5
2.4 E-2
Train B Interface Faults
H*X2
1.7 E-3

Figure G.10 Modularized Fault Trees for Events "HA*" and "HB*"

Table G.9 HPR

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

TOP EVENT **NOTES**

$$\mathrm{HPR} = \mathrm{L04} + (\mathrm{LOCA}\cdot \mathrm{H{*}1}\cdot \mathrm{H{*}01}) + \mathrm{HA}\cdot \mathrm{HB{*}} + \mathrm{HB}\cdot \mathrm{HA{*}} + \mathrm{HA{*}}\cdot \mathrm{HB{*}} + \mathrm{H{*}02}$$

$$\mathrm{HA{*}} = \mathrm{H{*}3} + \mathrm{H{*}2}\cdot \mathrm{H11} + \mathrm{H{*}X1}$$

$$\mathrm{HB{*}} = \mathrm{H{*}4} + \mathrm{H{*}5} + \mathrm{H{*}X2}$$

HA = see HPI Boolean equations
HB = " " " "

INTERMEDIATE EVENTS

$\mathrm{H{*}X1} = \mathrm{ACA{*}} + \mathrm{DCA{*}} + \mathrm{N{*}}$ 1

$\mathrm{H{*}X2} = \mathrm{ACB{*}} + \mathrm{DCB{*}} + \mathrm{DB{*}}$ 1

NOTES: 1. Offsite power is assessed to be recovered when entering the recirculation phase. The unavailability of AC power with offsite power available was calculated to be negligible compared to other system failure modes.

BEST DOCUMENT AVAILABLE

Table G.10 (1/2) Events "HPR", "HA*", and "HB*" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR-1)	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
H*3		TRAIN A VALVE FAULTS			2.0 E-3			
	VALVE DHV 11	FAILS TO OPEN	D		1.0 E-3	$3^+, 3^-$		
	CIRCUIT BKR 11	FAILS TO CLOSE	D		1.0 E-3	$3^+, 3^-$		
					Σ=2.0 E-3			
H*2		PUMP 1A FAILS TO RUN	1.0 E-3	24	2.4 E-2	$1^+, 30^-$	S	5, 1
H*4		TRAIN B VALVE FAULTS			2.0 E-3			
	VALVE DHV 12	FAILS TO OPEN	D		1.0 E-3	$3^+, 3^-$		
	CIRCUIT BKR. 12	FAILS TO CLOSE	D		1.0 E-3	$3^+, 3^-$		
					Σ=2.0 E-3			
H*5		PUMP 1C FAILS TO RUN	1.0 E-3	24	2.4 E-2	$1^+, 30^-$	S	5, 1
H11		PUMP 1B DOWN, PUMP 1A RUNNING AT ONSET OF INCIDENT			0.25			2
H*X1		TRAIN A INTERFACING SYSTEM FAULTS			1.0 E-5			
DCA*		DC POWER, TRAIN A FAULTS			ε			
ACA*		AC POWER, TRAIN A FAULTS			ε			
N*		FAILURE OF NUCLEAR SERVICES CLOSED CYCLE COOLING SYSTEM (NSCCCS) DURING RECIRCULATION			1.0 E-5			
H*X2		TRAIN B INTERFACING SYSTEM FAULTS			1.7 E-3			
DCB*		DC POWER, TRAIN B FAULTS			ε			
ACB*		AC POWER, TRAIN B FAULTS			ε			
DB*		FAILURE OF DECAY HEAT CLOSED CYCLE COOLING SYSTEM (DHCCCS), TRAIN B			1.7 E-3			
HA		SEE HPI FAULT TREE ANALYSIS			1.6 E-3			6
HB		SEE HPI FAULT TREE ANALYSIS			2.8 E-2			6
LO4		OPERATOR FAILS TO RECONFIGURE FOR RECIRCULATION	D		3.0 E-3	$10^+, 3^-$	0	3
H*02		OPERATOR INCORRECTLY RECONFIGURES FOR HIGH PRESSURE RECIRCULATION	D		8.0 E-2	$10^+, 10^-$	0	7

8448

Table G.10 (2/2) Event "HPR" Quantification

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
H*1· H*01		OPERATOR FAILS TO ISOLATE BREAK IN INJECTION LINE			1.0 E-3	3^+, 10^-	0	4
	INJECTION LINE (H*1)	BREAK OCCURS IN INJECTION LINE, GIVEN THAT SMALL BREAK OCCURS. ESFAS SIGNAL OCCURS AFTER RECONFIGURATION FOR RECIRCULATION FAILS TO CLOSE VALVES			0.1			
	OPERATOR (H*01)	FAILS TO CLOSE VALVE	D		1.0 E-2 *=1.0 E-3	3^+, 10^-	0	
LOCA		LOCA GATE						
		LOCA			1			
		NON LOCA			0			

284

BEST DOCUMENT AVAILABLE

Table G.10 HPR - Quantification Table

NOTES

1 The 24 hour run time for pumps during the recirculation phase represents an estimated nominal time after which corrective action could be assumed to mitigate failures that would prevent success during recirculation. This assumption corresponds to a similar assumption made in WASH 1400.

2 Pump 1B is assumed to be out of service for 3 months per year. Technical Specifications do not limit the outage time. It was conservatively assumed that the pump is not restored by the time recirculation is required.

3 This fault is assumed to be the same fault as a similar operator error that appears in the evaluation of the low head recirculation system.

4 The existence of this fault will depend upon whether or not an ESFAS signal (e.g., 500 psi primary pressure) is received after configuration for recirculation. This will depend on LOCA size within the smallest LOCA (B4) category. The assumed probability takes this into account. The fault applies to LOCA initiators only.

5 During recirculation, the high pressure pumps are required to pass sump water, which may contain concrete dust and other particulate matter. There is some question concerning the ability of the pumps to operate for extended periods of time in this environment, therefore the pump failure rate for extreme environments was used for the recirculation phase.

6 "Non-LOSP" values are used in HPR for HA and HB in all cases. For loss of offsite power transients, injection failures due to diesel failures are assumed to be recovered for recirculation. For events HA* and HB*, diesel failures therefore do not preclude "success during injection" as specified in the top event definitions.

7 This human error was evaluated using THERP tree analysis as described in NUREG/CR-1278.

Table G.11 HPR - Quantification Summary

BOOLEAN VARIABLE	POINT ESTIMATES
H*3	2.0 E-3
H*2	2.4 E-2
H*4	2.0 E-3
H*5	2.4 E-2
H11	0.25
H*X1	1.0 E-5
DCA*	ε
ACA*	ε
N*	1.0 E-5
H*X2	1.7 E-3
DCB*	ε
ACB*	ε
DB*	1.7 E-3
HA	1.6 E-3
HB	2.8 E-2
L04	3.0 E-3
H*1	0.1
H*01	1.0 E-2
H*02	8.0 E-2
LOCA	0* 1**

*non LOCA
**LOCA

APPENDIX H

CORE FLOOD SYSTEM (CFS)

APPENDIX H CORE FLOOD SYSTEM (CFS)

H.1 SYSTEM DESCRIPTION AND OPERATION

The core flood system is a passive engineered safeguards system which stores a supply of borated water which will automatically flow into the reactor vessel following a loss-of-coolant accident (LOCA). Although intended primarily to provide rapid core reflooding following a large LOCA, the tank contents will be injected into the reactor vessel any time the reactor coolant pressure drops below 600 psig. The CFS is required to operate only during the injection phase of accidents.

H.1.1 SYSTEM DESCRIPTION

The core flood system is depicted in the simplified schematic, Figure H.1. Each subsystem consists of a core flood tank containing at least 7626 gallons of borated water pressurized by 600 psig nitrogen, and three valves in the injection line path to the reactor vessel (RV). Instrumentation and alarms monitor tank pressure and level, and a relief valve provides overpressure protection. Each injection line path to the RV contains a normally open motor-operated valve (MOV) and two in-line check valves in series.

H.1.2 SYSTEM OPERATION

The core flood system is not dependent on any other system and requires no operator or control action to actuate. Since the core flood tank isolation MOV is normally open, the two check valves serve to prevent the high pressure reactor coolant from entering the core flooding tanks. Under a LOCA condition, these check valves open automatically when the reactor coolant system pressure drops below the 600 psig nitrogen pressure held in the tanks. To ensure that the MOV remains open, limit switches monitor the position of the MOV with annunication in the main control room. Additionally, the circuit breaker for the MOV motor control center is locked open. During operation, level and pressure are maintained when required by makeup from the High Pressure Injection System and nitrogen supply. Sample lines are provided to verify boron concentration periodically.

The following are general comments on limiting conditions for operation regarding the core flood system. For a more complete description refer to Section 3/4.5 of the Technical Sepcifications.

Each reactor coolant system core flooding tank must be operable with:

- the isolation valve open,
- a contained borated water volume between 7626 and 8005 gallons of borated water,
- between 2270 and 3500 ppm of boron, and,
- a nitrogen cover-pressure of between 575 and 625 psig.

The Technical Specifications require that if either a core flood tank is inoperable or the MOV closes, restoration must occur within 1 hour or go to a Hot Shutdown condition within the next 12 hours.

Surveillance requirements for the core flood system components include the following:

- Every 8 hours tank level and pressure as well as correct MOV position are verified.
- Every 31 days a sample is taken from the tanks to verify boron concentration.
- Every 31 days it is ensured that no power is available to the valve actuator by verifying the associated breaker is locked open.
- Every 18 months (prior to shutdown for refueling) the core flood "Isolation Valve Closed" alarm is verified to annuciate when the MOV is not fully open. During this same period as plant cooldown continues and reactor coolant pressure drops, the in-line check valves are verified to actuate by observing pressurizer level and core flood tank level.

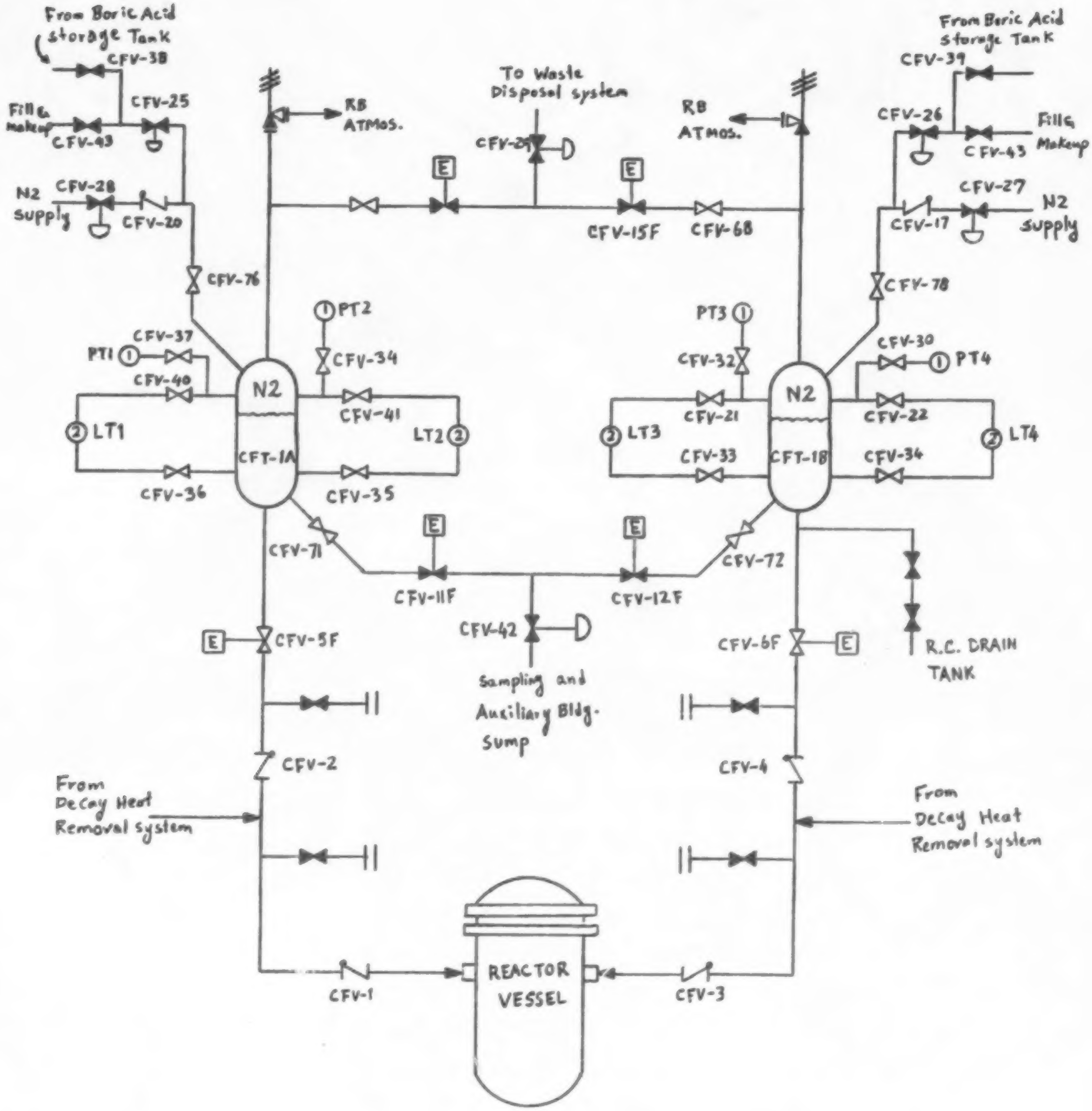

From Boric Acid storage Tank
CFV-38
Fill & makeup
CFV-43
CFV-25
N2 supply
CFV-28
CFV-20
CFV-76
RB ATMOS.
To Waste Disposal system
CFV-29
E
CFV-15F
CFV-68
RB ATMOS.
From Boric Acid Storage Tank
CFV-39
CFV-26
Fill & Makeup
CFV-43
CFV-27
N2 Supply
CFV-17
CFV-78
PT1
CFV-37
CFV-40
LT1
CFV-36
N2
CFT-1A
PT2
CFV-34
CFV-41
LT2
CFV-35
PT3
CFV-32
LT3
CFV-21
CFV-33
N2
CFT-1B
CFV-30
PT4
CFV-22
LT4
CFV-34
CFV-71
CFV-11F
CFV-12F
CFV-72
CFV-42
Sampling and Auxiliary Bldg. Sump
CFV-5F
CFV-6F
R.C. DRAIN TANK
CFV-2
CFV-4
From Decay Heat Removal system
From Decay Heat Removal system
REACTOR VESSEL
CFV-1
CFV-3

Figure H.1 Core Flood System Schematic Diagram

H.2 SYSTEM SIMPLIFIED FAULT TREE

The FSAR Section 14 indicates that both core flood systems are required for a large LOCA. However, the fault tree is drawn with house events in order to be representative whenever one or both systems are required. Loss of one core flood system is represented by single faults associated with pipe ruptures, check valves failing to open, MOV plugging, and inadvertent actuation of the core flood tank relief valve. As noted on the fault tree, inadvertent opening of the relief valve with failure to reseat would be immediately detectable by the associated tank level and pressure instrument alarms. Common mode failures were considered for operator error during initial fill and pressurization of the tanks as well as incorrect boron concentration. The first two should be considered unlikely since instrumentation monitors tank level and pressure. However, an additional common mode event was considered for miscalibration of this instrumentation by maintenance personnel which could result in insufficient volume or pressure.

Figure H.2 shows the simplified fault tree for the CFS.